



DPC: 25/30452710 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 20 January 2025

Origin: International

Latest date for receipt of comments: 15 March 2025

Project No. 2022/00438

Responsible committee: IST/35 Health informatics

Interested committees:

Title: Draft BS EN ISO 27799 Health informatics — Information security management in health using ISO/IEC 27002.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 15 March 2025

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



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)

Full document details: 25/30452710 DC

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

© ISO 2025



Documents

Document Sharing Hub



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	14
5.29 Information security during disruption	15
5.30 ICT readiness for business continuity	15
5.31 Legal, statutory, regulatory and contractual requirements	15
5.32 Intellectual property rights	15
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	17
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.....	22
6	People controls.....	22
6.1	Screening.....	22
6.2	Terms and conditions of employment.....	23
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

ISO/DIS 27799:2025(en)

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		73

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:

- indicates which controls (including their purposes, guidance and any other information) in ISO/IEC 27002:2022 apply unchanged in health;
- for certain controls in ISO/IEC 27002:2022: provides guidance, other information, or both on how to apply the controls in health;
- 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;
- 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;

- b) the goals of health information security;
- c) compliance scope;
- d) legislative, regulatory, and contractual requirements, including those for the protection of personal health information and the legal and ethical responsibilities of health professionals to protect this information;
- e) arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentiality, without fear of blame or recrimination;
- f) the importance of reporting actual or suspected incidents including near misses as soon as possible so that any incidents that do occur can be dealt with at the earliest opportunity and do not become more serious;
- g) the identification of processes and systems that are vital in healthcare (that is failure can lead to adverse effects in care or to reduced patient safety).

Revision of the policy's contents should be driven by the findings of a risk assessment.

In creating and maintaining the information security policy document, the following factors should be considered:

- a) the breadth of health information;
- b) the rights and responsibilities of staff, which include legal and ethical requirements, standards set by professional bodies, and any local requirements;
- c) the rights of subjects of care to privacy and, where applicable, to access to their records;
- d) the obligations of clinicians with respect to obtaining informational consent from subjects of care and maintaining the confidentiality of personal health information;
- e) multiple organisations (which can be in different jurisdictions from each other) providing healthcare or supporting services, as well as individuals (including the subjects of care themselves and their relatives or close companions) can be involved in the current or past delivery, determination, administration or funding of a subject's health and social care (see [Annex C](#));
- f) the protocols and procedures to be applied to the sharing of information for the purposes of research and clinical trials;
- g) the arrangements for and access limits of
 - 1) personnel involved in the delivery of care, including permanent and temporary or visiting staff such as locums, trainees, students and “on-call” or agency staff (see [Annex C](#) for further information);
 - 2) personnel who are supporting direct care, including administrative and support staff as well as clergy, charity workers and other volunteers (see [Annex C](#) for further information);
 - 3) personnel from regulatory and inspection bodies, financial and other auditors, health professionals and others investigating clinical or other incidents involving care provisioning;
- h) situations where information about a subject must be provided externally or is requested by authorities or other third parties: such situations can include where someone has been harmed during a crime, when there is suspected abuse or inadequate care of children, women, elderly, learning-impaired or other vulnerable subjects of care;
- i) the implications of security measures on patient safety;
- j) the implications of information security measures on the functionality and performance of health information systems.

Where support from or collaboration with third parties is obtained, and especially where it receives services from other jurisdictions, the policy framework should include documented policy and procedures that cover such interactions and specify the responsibilities of all parties.

Where applicable, reviews of policies should address:

- a) the changing nature of operations and the concomitant changes to risk profile and risk management needs;
- b) the changes made to the ICT architecture and/or infrastructure, and the concomitant changes these bring to the risk profile;
- c) the changes identified in the external environment that similarly impact the risk profile;
- d) the latest controls, compliance and assurance requirements and arrangements mandated by jurisdictional health bodies or by new legislation or regulation;
- e) the latest guidance and recommendations from health professional associations and from supervisory authorities in the field of protection of personally identifiable information (see also [5.34](#));
- f) the results of legal cases tested in the courts, which have established or negated precedents or established practices;
- g) the challenges and issues regarding the policy, as expressed to the organization by its staff, subjects of care and their partners and care givers, researchers and governments (e.g., supervisory authorities in the field of protection of personally identifiable information);
- h) reports on patient safety incidents in order to devise mitigations in those cases where the patient safety incident is the result of failures of information security measures.

5.2 Information security roles and responsibilities

Control [5.2](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

There should be at least one individual responsible for information security.

Purpose (supplementary)

To ensure that there is clear direction, visible management support for activities involving the security of health information and adequate technical expertise.

Guidance for health

Accountability and coordination of information security can only be maintained over the long term if the organization has an explicit information security management infrastructure.

An important element in roles and responsibilities with regard to information security is the presence of, or access to, an information security officer, who is responsible for the coordination of information security. Of paramount importance is the accountability of top management for all things related to information security.

Many organizations and particularly larger ones (for example, with a workforce of more than 500 or a client base of more than 10 000) should have an information security advisory group. Such groups are sometimes termed committees or boards.

The group's purpose is to ensure that there is clear direction and visible management support for ensuring the security of health information. The group should meet regularly, typically on a monthly basis, to 'stay on top of things' and keep up-to-date.

In addition to the information security officer, the group should include representatives from the organization who:

- use health IT systems or other ICT infrastructure and services (for example, doctors, nurses, other clinicians, managers, administrators)
- have professional responsibility or accountability within the organisation for the operation of the systems and services (for example, ICT staff, medical device and hospital engineering professionals).

Other information for health

See [Annex C](#) for further information on information security advisory groups.

5.3 Segregation of duties

Control [5.3](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

In very small organizations, it is sometimes not possible to segregate all conflicting duties and areas of responsibility. In such cases, duties and areas of responsibility should be segregated where feasible. Additionally, measures should be considered where problematic conflicts remain. The remaining areas of conflict should be documented along with the compensatory measures.

Many staff in healthcare, such as professionals and researchers, switch roles continuously. What isn't a conflicting duty or area of responsibility, can easily become one in an instant. For example, a physician is at one moment supervising a doctor in training and at the next moment administering care. Special consideration should be given to segregation of duties and areas of responsibility where roles change frequently.

5.4 Management responsibilities

Control [5.4](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.5 Contact with authorities

Control [5.5](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.6 Contact with special interest groups

Control [5.6](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Privacy requirements can have significant implications for security. Because of the special considerations that apply in healthcare, involvement with groups, forums and professionals' associations that have a specific focus on the privacy and security of health information should be considered.

5.7 Threat intelligence

Control [5.7](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

In health, there is a wide range of threats to be taken into account and for which intelligence should be maintained. Factors that are particularly relevant include the following:

- a) In addition to generic ICT and Internet-of-Things devices, there is equipment specific to health, including many different types and models of medical devices.
- b) On generic ICT equipment, security measures include updating software, applying patches and using software that protects against malware. For clinical safety and other reasons, there can be restrictions on taking measures such as these on some medical devices incorporating health software.
- c) Many health organizations use hardware and software that is obsolete, inappropriately configured, or both.
- d) There can be particular challenges with maintaining accurate inventories and controlling assets.

Other information for health

See [Annex C](#) for further information.

5.8 Information security in project management

Control [5.8](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Safety and privacy should be considered in project management.

Other information for health

See also [5.38](#) which considers analysis and specification. See also [5.34](#) which address privacy.

ISO 81001-1 provides extensive guidance on the interdependency of safety, effectiveness and security including project management issues. ISO 81001-1 also provides information on other relevant standards, particularly for medical devices.

5.9 Inventory of information and other associated assets

Control [5.9](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

All information flows (both within and between organizations) and their interfaces (including integration platforms), should be included in the inventory.

Purpose for health (supplementary)

To ensure that information flows and their interfaces are identified in order to preserve their information security and assign appropriate ownership.

Guidance for health

Besides assets such as equipment, devices and software components, health organizations increasingly become dependent on structural information flows (between areas within the organization's IT-landscape but also with outside parties) and associated interfaces, especially integration platforms.

Ownership can, at times, be difficult to determine in client-supplier situations. In such cases, the (contractual) agreement between parties can offer help; this also assists in establishing owner duties.

Other information for health

See [Annex C](#) for further information on asset ownership as well as the different types and uses of assets.

5.10 Acceptable use of information and other associated assets

Control [5.10](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.11 Return of assets

Control [5.11](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

There should be a policy that requires written confirmation from individuals that all assets in their possession in all formats have been securely returned or deleted as appropriate.

Purpose for health (supplementary)

To protect personal health information as part of the process of changing or terminating employment, contract or agreement.

Guidance for health

The policy should include measures that can be taken against individuals if it is found, during or subsequent to change or termination of employment, contract or agreement, that not all assets have been returned or deleted as appropriate.

The written confirmation required by the policy should include all information that does not belong to an individual and that is held on their own personal equipment or held on the individual's behalf elsewhere (for example, storage and other services, including email, provided by cloud providers).

In cases where returning information held by an individual or on their behalf would result in unnecessary duplication, the policy may allow the individual to delete the information securely without returning it. The policy should stipulate the techniques to be followed to ensure secure deletion.

5.12 Classification of information

Control [5.12](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

Personal health information should be classified as confidential at a minimum.

Purpose for health (supplementary)

To ensure the proper classification of personal health information under all circumstances.

Guidance for health

Classification in healthcare can be challenging. The following factors should be taken into consideration.

- Legal, statutory, regulatory, contractual and local policy requirements for medical records and other personal health information vary significantly. In some cases the requirements are based on rules for paper records and do not take sufficient account of information being held electronically. Other potential issues are unclear or inconsistent requirements. This often happens because requirements are constantly evolving and because there can be multiple sources of requirements. For example, PHI, as a subset of PII, can be governed by overarching general data protection legislation as well as other requirements that are not specific to health.
- Within the realm of personal health information, it can be necessary to have a range of classifications. For example, information on a broken leg is clearly of a different degree than that regarding sexually transmitted diseases. There can be varying degrees between personal health information of a high-

profile person with respect to that of other persons. Other degrees can evolve over time: some personal data can be less sensitive (for example, the difference between a mental health episode ten years ago vs. a current one), while others can become more sensitive. Personal information can also become enriched with data from other sources, changing its classification. In addition, some personal health information can point to other persons: for example, family members with regard to genetics, or people with regard to harm they have inflicted (for example, in cases of child abuse).

Personal health information, all of which should be classified, can also come from wearable technology, implants and other medical devices.

5.13 Labelling of information

Control [5.13](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Not all health information is confidential and not all health information systems provide users with access to personal health information. Users of health information systems need to know when the data they are accessing contain or constitute personal health information.

Consideration should be given to informing users, e.g., at each start up or log in. However, it can be sufficient to provide such information only the first time a particular user accesses a system.

5.14 Information transfer

Control [5.14](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

Rules, procedures and agreements should be in place prior to any transfer taking place.

Purpose for health (supplementary)

To ensure security of information transfer over its full life cycle.

Guidance for health

Organizations should ensure that the security of information exchange is the subject of policy development and compliance audit (see [5.36](#)). Cryptographic techniques should be used appropriately.

The security of information exchanges can be greatly assisted by the use of information exchange agreements that specify the minimum set of controls to be implemented. Such agreements are binding on both (or more) information exchanging parties, whereas rules and procedures are generally only applicable within a single organization.

Policies should be in place to ensure that personal health and other confidential information exchanged over e-mail, instant messaging or in other forms is secure. If sufficient security cannot be achieved, such information should not be exchanged through these channels at all.

Other information for health

Specific guidance on health information exchange policies can be found in ISO 22857. Though ISO 22857 explicitly references trans-border flow of personal health information (where borders in this context represent legal domains, not necessarily national boundaries), much of its advice can be adapted, where necessary, to deal with the exchange of data from one organization to another.

5.15 Access control

Control [5.15](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

Access to personal health information should be governed by a role-based access control policy.

Purpose for health (supplementary)

To ensure access based on well-established roles.

Guidance for health

Role-based access control

The role-based access policy should:

- a) be established on the basis of predefined roles with associated authorities that are consistent with, but limited to, the needs of that role;
- b) reflect professional, ethical, legal and subject-of-care-related requirements; and
- c) take account of the tasks performed by health professionals or other authorized personnel and the task's workflow.

Control of access to personal health information

Access to personal health information should be controlled. In general, users of health information systems should only access personal health information:

- a) when the user is part of the care team of the data subject (the subject of care whose personal health information is being accessed);
- b) when the user is carrying out an activity on behalf of the data subject;
- c) when there is a need for specific data to support this activity.

In order to prevent healthcare delivery being delayed or otherwise adversely affected, a clear policy and process, with associated authorization, to override the “normal” access control rules in emergency situations (sometimes referred to as ‘break the glass’) can be necessary.

Other information for health

See also [5.34](#) on additional privacy considerations that can restrict access to personal health information and should be included as appropriate in the access control policy.

The ISO 22600 series provide further information on access control in health informatics.

5.16 Identity management

Control [5.16](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

Users who are to have access to personal health and other confidential information should be subject to a formal registration process.

Purpose for health (supplementary)

To ensure that each individual is allocated a correct user identity.

Guidance for health

The registration process should include rigorous checks to ensure that the identities allocated to users will be both subject to appropriate authentication and their access rights are consistent with their roles.

The registration process should, where applicable, include all of the following:

- a) checking that the individual is who they claim to be;
- b) verification of the individual's professional credentials, including whether they are currently valid;
- c) accurate capture of the information associated with the individual;
- d) assignment of a unique and unambiguous user identity.

For personnel who are new to an organization, the personal details - such as name, date of birth – should be checked against a suitable document such as a passport unless this has been done as part of the screening process (see [6.1](#) for further information).

The registration process should accommodate varying types of users including health professionals, ICT staff with elevated rights, subjects of care and their support companions, all of whom have different registration prerequisites.

Other information for health

It can be beneficial to coordinate identity management with activities relating to physical security. An example is the allocation of security passes that control access to rooms or locations. Another example is the allocation of identity badges or passes.

5.17 Authentication information

Control [5.17](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Time pressures found in health delivery situations can make effective use of passwords difficult to employ. Health organizations should in such cases consider the adoption of alternative authentication technologies to address this problem.

Other information for health

See also [8.5](#).

5.18 Access rights

Control [5.18](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health**Consideration before change or termination of roles**

Especially in large hospitals, significant numbers of staff will typically have short-term access to personal health information. The termination of the access rights of such staff needs to be carefully managed. Examples of such staff include students, interns, trainees and locums. Other examples include agency or equivalent staff, as well as permanent employees providing cover for other people's roles or shifts.

Another issue is that many transactions take place sometime after care events (e.g., the sign-off of medical transcriptions) and in some cases the transactions take place a considerable time later. This can significantly complicate the process of removing access rights in a timely fashion and these transactions should be taken into account when designing and implementing procedures on the removal of access rights.

Immediate termination of access rights following the supply of a resignation notice, notice of dismissal, etc. should be considered, wherever an increased risk is perceived from the continuation of such access.

5.19 Information security in supplier relationships

Control [5.19](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

The risks associated with access by external parties to systems or the data they contain, should be assessed and controls that are appropriate to the assessed risk, should be implemented.

Purpose for health (supplementary)

To manage and protect the external access of suppliers to systems and data.

Guidance for health

Risk assessment is essential for effectively managing third-party access to systems containing health information, especially personal health information.

Rights of subjects of care should be protected, even when a third party with potential access to personal health information is located in a jurisdiction different than the one governing the subject of care or health organization.

All personal health and other confidential information that could be accessed by suppliers for whatever reason, including provision of cloud services, processing, support, training or testing, should be encrypted.

There should be policies together with processes and procedures to ensure this is achieved and monitored. In some cases, for example certain medical devices, it is not possible to encrypt data and compensating controls based on a risk assessment should be implemented instead.

Other information for health

Depending on the systems, services and suppliers, information can potentially be accessed in many ways including use of application programs or utilities and tools that operate, for example, on databases, file systems or networks. Suppliers and their subcontractors can have administrative or other rights as well as diagnostic or privileged utilities that could enable or provide access to confidential information. It is difficult, if not impossible, for clients of suppliers to know the full extent of suppliers' capabilities. These factors should be taken into account when assessing risks with supplier relationships.

5.20 Addressing information security within supplier agreements

Control [5.20](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.21 Managing information security in the ICT supply chain

Control [5.21](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

For medical devices incorporating health software the information that should be provided by manufacturers includes: a disclosure statement for Medical Device Security (MDS2), configuration requirements, vulnerability assessments and a software bill of materials (SBOM).

Other information for health

See [Annex D](#) and ISO 81001-1.

5.22 Monitoring, review and change management of supplier services

Control [5.22](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.23 Information security for use of cloud services

Control [5.23](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Other information for health

ISO/TS 23535 and ISO/TR 21332 provide information on security and privacy for cloud services used in health.

5.24 Information security incident management planning and preparation

Control [5.24](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Information security incidents should not be assessed in isolation from other types of incidents, both in handling and in reporting. All types of incidents should be included in the information security incident management process. After all, a break-in could have led to theft of ICT hardware (leading to a confidentiality breach), or a fire could have been set to disguise misuse of ICT equipment, or an identified misuse or erroneous use of the system could have had clinical consequences, etc.

5.25 Assessment and decision on information security events

Control [5.25](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

The categorization and prioritization scheme should consider whether events involved either or both:

- a) personal health information;
- b) medical devices incorporating health software.

The scheme should also consider whether clinical activities were (potentially) affected.

5.26 Response to information security incidents

Control [5.26](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.27 Learning from information security incidents

Control [5.27](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.28 Collection of evidence

Control [5.28](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Health organizations should consider the implications of collecting evidence for purposes of investigating clinical incidents.

5.29 Information security during disruption

Control [5.29](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.30 ICT readiness for business continuity

Control [5.30](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Organizations should identify processes, systems and other relevant equipment that are vital in healthcare delivery.

Fall-back procedures should be considered as necessary in order to counter failure in processes, systems and other relevant equipment that are vital in healthcare delivery.

Reflecting the rigorous availability requirements in healthcare, particular attention should be paid to resilience and redundancy arrangements, both for technology as well as for personnel.

ICT continuity planning in healthcare should be suitably integrated within business continuity planning (e.g., plans for handling power failures, implementing infection control and dealing with other clinical emergencies).

The safety of subjects of care can depend upon access to their data and it is essential that this be taken into account during planning. Catastrophes and force majeure crises that would disable ICT systems in industrial and other sectors are the very events that can precipitate a health crisis in which timely access to health information is crucial.

Health organizations also need to ensure that the plans that they develop are regularly tested on a “programmatic” basis. The tests included in that programme should build upon one another, proceeding from desktop testing to modular testing to synthesis of likely recovery times and then finally to full rehearsals. Such a programme is thus low risk and delivers real improvement in the general level of awareness in its user population.

Health organizations should remain cognizant of the role that health information systems play in continuity of care. Such organizations should be prepared if/when ICT systems fail.

Depending on the nature and duration of a system outage, it can be necessary to capture by other means data about subjects of care that would be recorded in the system under normal circumstances. Backup arrangements can include, for example, use of spreadsheets or paper forms. Contingency arrangements should ensure that information captured during outages is as accurate, complete and timely as possible.

Data captured during an outage will often need to be transferred or entered manually into systems once they are running again after the outage. Additional checks for accuracy, completeness and data integrity should be performed as part of the update processes.

5.31 Legal, statutory, regulatory and contractual requirements

Control [5.31](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.32 Intellectual property rights

Control [5.32](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.33 Protection of records

Control [5.33](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.34 Privacy and protection of PII

Control [5.34](#), the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Access to personal health information should only be permitted where the user has a legitimate need to access a subject of care's records.

Where the user has a legitimate need, this does not necessarily mean the user is entitled to access all the subject of care's personal health information because legal, regulatory, professional, local policy or other requirements can result in additional access restrictions. For example:

- a) access to personal health information concerned, for instance, with a subject of care's sexual health, mental health, contraception, any current pregnancy or the outcomes of any previous pregnancies can be restricted to the clinicians treating the specific conditions;
- b) subjects of care can have rights to specify which of their health records are either accessible or not to particular users or groups of users;
- c) subjects of care can have rights to access their own records but there can be requirements to withhold some information from them; this can apply to some mental health conditions or where there is information in a subject of care's health records about other individuals, such as relatives with related conditions or diagnoses, whose privacy has to be protected;
- d) when certain health matters such as those listed in a) are being recorded, subjects of care can be given records under aliases or special identifiers and access to their true identification information is restricted;
- e) certain subjects of care can be given aliases or special identifiers for all their records to prevent access to their true identities; this can apply, for example, to 'very important persons' (VIPs), members of the security forces and victims of crime.

Additional considerations apply to access to records of children or adults who have proxies.

In cases where subjects of care or their proxies have rights to specify whether access to particular records should be granted or denied, suitable logs should be maintained. These logs should include details of advice given to subjects of care or their proxies and the decisions they subsequently take.

There are options for when access to part of a subject of care's records is denied. For example:

- a) the information in question can be hidden altogether, so that the user is not shown that it is there at all;
- b) the information can be obscured or it can be replaced with text informing the user that certain information is restricted.

Legal, regulatory or local policy requirements should be followed to determine the appropriate actions when denying access. Methods for denying access are considered in [8.11](#).

As noted in [5.15](#), it can be necessary to override certain access controls or restrictions in emergencies.

Special emphasis should be placed on the concerns of subjects of care who do not wish their personal health information to be accessed by health workers who are neighbours, colleagues, or relatives. Likewise, staff members often do not wish to be placed unnecessarily in the position of reviewing information about friends, relatives, or neighbours. Effective management of health information systems should address these concerns.