DRAFT International Standard

ISO/DIS 27799

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

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

ICS: 35.030; 35.240.80

ISO/TC **215**

Secretariat: **ANSI**

Voting begins on:
2025-01-20

Voting terminates on:
2025-04-14

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/DIS 27799:2025(en)

COPYRIGHT PROTECTED DOCUMENT

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

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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

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

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

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

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

The main changes are as follows:

— alignment with the new structure of ISO/IEC 27002:2022 and other changes to that standard from the previous version

— revision and addition of controls specific to health

— removal of material that is in ISO/IEC 27002:2022 but was not in the previous version of that standard.

— addition of informative Annexes providing i) supplementary guidance on cybersecurity in health organizations and ii) example security and privacy requirements for health information systems.

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

Introduction

0.1 General

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

0.2 Context and Background

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

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

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

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

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

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

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

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

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

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

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

0.3 Audience and Uses

This document is targeted at organizations that:

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

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

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

Individuals for whom this document is particularly relevant include:

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

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

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

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

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

1 Scope

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

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

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

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

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

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

3 Terms, definitions and abbreviated terms

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

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

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

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

3.1 Terms and definitions

3.1.1
health
complete physical, mental and social well-being

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

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

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

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

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

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

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

Note 1 to entry: Personal health information may include:

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

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

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

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

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

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

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

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

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

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

EXAMPLE 1 Parents of children who are not yet adults.

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

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

3.2 Abbreviated terms

HLT health

ICT information and communication technology

ISMS information security management system

PII personally identifiable information

4 General

4.1 Structure of this Document

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

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

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

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

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

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

This document contains 4 Annexes:

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

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

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

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

4.2 Safety

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

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

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

4.3 Selecting and applying controls

4.3.1 Determining controls

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

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

4.3.2 Application of Guidance

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

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

4.3.3 Use with ISO/IEC 27001:2022

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

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

5 Organizational controls

5.1 Policies for information security

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

Control for health (supplementary)

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

Purpose for health (supplementary)

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

Guidance for health

The information security policy should contain statements on:

a) the need for health information security;

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.

Other information for health

Further information on the management of information consent in healthcare can be found in ISO/TS 17975.

ISO/IEC 27701 is an extension to ISO/IEC 27001 and ISO/IEC 27002 that provides requirements and guidelines for privacy information management. Many of the controls can be applied in health.

See also Annex D.

5.35 Independent review of information security

Control 5.35, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Because of the specialized nature of healthcare, including the interdependencies between safety and information security, the use of independent reviewers with an understanding of the sector should be considered.

Although not necessarily performed by relevant experts and not strictly independent, assessment by colleagues from a peer organization can act as a useful supplement to formal independent reviews.

5.36 Conformance with policies, rules and standards for information security

Control 5.36, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

A compliance auditing programme should be in place that addresses the full life cycle of operations, that:

a) identify issues,

b) review outcomes, and

c) decide on updates to the ISMS.

The audit programme should be formally structured within a 12- to 18-month cycle, to cover:

a) all elements of this document,

b) all areas of risk, and

c) all implemented controls.

Where applicable, the information security advisory group (see 5.2) should set itself the objective of establishing a graduated compliance auditing framework, whose bottom layer is self-audit by the process operators and managers. Thereafter, the auditing of the ISMS, on behalf of the information security advisory group, internal auditing, controls assurance assessments and finally external audits, should be defined in a manner that allows each layer to draw confidence from all of the layers below it.

5.37 Documented operating procedures

Control 5.37, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

5.38 HLT – Information security requirements analysis and specification

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Continuity	#Protection, #Defence, #Resilience

Control

The information security-related requirements should be included in the requirements for new information systems or enhancements to existing information systems.

Purpose

To ensure information security risks related to the development and/or acquisition of information systems are effectively addressed throughout the information system life cycle.

Guidance

Information security requirements should be identified using various methods such as deriving compliance requirements from policies and regulations, threat modelling, incident reviews, or use of vulnerability thresholds. Results of the identification should be documented and reviewed by all stakeholders.

Information security requirements and controls should reflect the value of the information involved (see 5.12 and 5.13) and the potential negative impact that might result from lack of adequate security. The implications for safety should also be considered.

Identification and management of information security requirements and associated processes should be integrated in the early stages of information systems projects. Early consideration of information security requirements, e.g., at the design stage can lead to more effective and cost-efficient solutions.

Information security requirements should also consider:

a) the level of confidence required towards the claimed identity of users, in order to derive user authentication requirements;

b) access provisioning and authorization processes, for all types of users including privileged or technical users;

c) informing users and operators of their duties and responsibilities;

d) the required protection needs of the assets involved, in particular regarding availability, confidentiality, integrity;

e) requirements derived from operational processes, such as transaction logging and monitoring, nonrepudiation requirements;

f) requirements mandated by other security controls, e.g., interfaces to logging and monitoring or data leakage detection systems.

For applications that provide services over public networks or which implement transactions, the dedicated control 8.26 should be considered.

If products are acquired, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls should be reconsidered prior to purchasing the product.

Available guidance for security configuration of the product aligned with the final software / service stack of that system should be evaluated and implemented.

Criteria for accepting products should be defined (for example, in terms of their functionality), which will give assurance that the identified security requirements are met. Products should be evaluated against these criteria before acquisition. Additional functionality should be reviewed to ensure it does not introduce unacceptable additional risks.

Other information

See Annex D.

ISO/IEC 27005 provides guidance on the use of risk management processes to identify controls to meet information security requirements.

5.39 HLT – Uniquely identifying subjects of care

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Continuity	#Protection, #Defence, #Resilience

Control

There should be policies and procedures to ensure there is a single unique identifier for each subject of care, and functionality to merge duplicate or multiple records in cases where they exist for the same subject of care.

Purpose

To prevent incomplete or inconsistent information and records about subjects of care.

Guidance

Emergency care and other situations in which adequate identification of a subject of care has not been possible can result in instances of multiple records for the same subject of care. In addition, subjects of care can have multiple records for administrative reasons such as the merger or takeover of previously separate health organizations at which they have been treated.

Health information systems should have the facility to merge multiple records for a subject of care into a single record. Such merging requires the greatest care and will therefore not only necessitate personnel trained in such merging, but can also require technical tools to facilitate the integration of information from the original records into a unified whole.

Organizations processing personal health information should ensure that data from which personal identification can be derived are only retained where it is necessary to do so and that deletion, anonymization and pseudonymization techniques are appropriately used to the full extent possible to minimize the risk of unintentional disclosures of personal information.

5.40 HLT – Validation of displayed/printed data

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Continuity	#Protection, #Defence, #Resilience

Control

When any of an individual's personal health information is displayed or printed, information that identifies the subject of care should be included.

Purpose

To enable confirmation that information is for the correct subject of care and to prevent use of information that relates to someone else.

Guidance

Before relying on personal health information provided by a health information system, health professionals need to be shown sufficient information to ensure that the subject of care they are treating matches the information presented. Matching a subject of care under treatment to an existing record can be a non-trivial task. Some systems enhance security by including photographic identity with each subject of care's record. Such enhancements can themselves create privacy problems, as they potentially permit the implicit capture of facial characteristics, such as race that are not included as fields of data. The requirements for identification of subjects of care and the availability of data used to support it can also vary from jurisdiction to jurisdiction. Great care needs to be exercised in the design of health information systems to ensure that health professionals can trust the system to provide the information needed to confirm that each record retrieved matches the individual under treatment.

Health information systems should make it possible to check that hardcopy print-outs are complete (for example, page 3 of 5).

5.41 HLT – Publicly available health information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Integrity	#Protect	#Governance, #Asset_management, #Information_protection, #Legal_and_compliance	#Protection, #Defence

Control

Publicly available health information should be protected, traceable, preserved and managed throughout its lifecycle.

Purpose

To ensure publicly available health information is available when required, its integrity is maintained, its provenance is recorded, there is an audit trail, and historical information is retrievable.

Guidance

Publicly available health information (as distinct from personal health information) can be found at websites and, for instance, in portals. It can often take the form of medical advice. For instance, information on when to make an appointment with a doctor, midwife or other clinician, as opposed to visiting the emergency department immediately. Information, including side-effects, on prescription and other medications is also often publicly available along with explanations of the diagnosis and treatment of many conditions.

Important decisions can be made by subjects of care, their companions or proxies based on publicly available health information. Health professionals can also rely on such information. It is therefore essential that publicly available health information is reliable, accurate and up-to-date. To ensure this:

a) the integrity and availability of the information should be protected;

b) the origin of the information should be stated and its provenance should be checked before it is made available;

c) there should be a full audit trail so it is evident which personnel created, amended, deleted or performed other actions on the information;

d) a comprehensive archive of the information should be maintained and there should be a facility to access the historical information in order to establish what content was available at any particular time.

Other information

Similar principles should be applied for information on intranets, internal knowledge bases and similar resources that are only available to personnel within an organisation.

5.42 HLT – Emergency communication

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Availability	#Respond, #Recover	#Governance, #Information_protection, #Human_resource_security, #Threat_and_vulnerability_management, #Continuity, #Supplier_relationships_security, #Information_security_event_management, #Information_security_assurance	#Protection, #Defence, #Resilience

Control

Emergency communication channels within a health organization that function when the organization's ICT continuity has failed, should be planned, implemented, maintained and tested.

Purpose

To ensure that essential communications are possible during an ICT outage.

Guidance

Interpersonal communication increasingly uses ICT, resulting in a corresponding increase in dependence on ICT. If there is an ICT failure, communication using ICT will quickly become impossible. That is not acceptable for providing care. Therefore, emergency communication that does not rely on (organizational) ICT must be planned, implemented, maintained and its effectiveness tested regularly. For instance, mobile communication can be used instead of network communication, and paper forms can be used to communicate pathology requests and results.

5.43 HLT – External incident reporting

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective, #Corrective	#Integrity, #Availability	#Respond	#Governance, #Threat_and_vulnerability_management, #Supplier_relationships_security, #Legal_and_compliance	#Governance_and_Ecosystem

Control

Information security incidents should be reported in accordance with legal, statutory, regulatory or contractual obligations.

Purpose

To ensure that legal, statutory, regulatory and contractual obligations regarding information security incidents are met.

Guidance

In healthcare and elsewhere, the need for reporting information security incidents to authorities and/or contractual partners is growing. It enables such parties to quickly uncover patterns in cybercrime. To ensure that such reporting obligations are met, it is necessary to first perform an inventory of such obligations. Based on this:

a) parties within the organization should be appointed who are responsible for (groups of) individual reports, and

b) the scope (length and breadth) of each report should be established based on a balance between reporting requirements and the protection of personal (health) information.

Every time an external incident report has been submitted, management should be informed of this.

Other information

See also 5.31.

6 People controls

6.1 Screening

Control 6.1, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

All organizations where personal health information is processed should have a policy for screening personnel. As a minimum, the policy should require verification of identity, current address and previous employment.

Background checks on all candidates to become personnel should include a verification of applicable health professional qualifications and, where applicable, that they are accredited or licensed to practice. Where applicable, criminal background checks should be undertaken. All checks should be repeated regularly.

6.2 Terms and conditions of employment

Control 6.2, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

Job descriptions should state the security roles and responsibilities that apply to processing of personal health information.

Purpose for health (supplementary)

To ensure privacy of subjects of care is emphasized and understood.

Guidance for health

Organizations should ensure that personnel have a duty to report breaches of health information security or subject of care privacy.

Policies need to address all types of personnel whether permanent or not, including:

a) clinicians who are temporary or visiting such as locums, trainees, interns, students and “on-call” or agency staff;

b) personnel who are supporting direct care, including administrative and support staff as well as clergy, charity workers and other volunteers.

Other information for health

See Annex C for further information on the workforce in health organizations.

6.3 Information security awareness, education and training

Control 6.3, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Awareness, education and training can include regular assessment and/or testing.

6.4 Disciplinary process

Control 6.4, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

The disciplinary process should state (both as a deterrent and because it can be necessary) that, for serious violations, individuals will be reported to one or more external bodies.

For example, clinicians could be reported to their regulatory or registration body. Students and trainees could be reported to the academic institution they are associated with.

6.5 Responsibilities after termination or change of employment

Control 6.5, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Many doctors, nurses and other clinicians progress through training programmes and other 'rotations' where their clinical duties, and the subjects of care they are involved in the care of, can change fundamentally.

To ensure the termination of access and any associated rights that are no longer required for their role, changes of employment should be initially processed in the same way as for individuals who are leaving the organization's employ.

Other information for health

Changes of employment can also affect the physical locations that individuals are able or permitted to access. Arrangements should be in place to ensure suitable changes to security passes and/or other measures for physical and premises security.

See 5.15 and 5.18 for situations regarding temporary staff.

6.6 Confidentiality or non-disclosure agreements

Control 6.6, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

All personnel authorized to access personal health information should be formally bound to treat such information confidentially.

Purpose for health (supplementary)

To formally maintain confidentiality of information accessible by personnel or third parties.

Guidance for health

A formal binding can, for instance, come from a signed agreement such as a non-disclosure, regulatory requirements, or confidentiality agreement, or from law.

6.7 Remote working

Control 6.7, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Other information for health

In healthcare, working remotely can cross jurisdictional borders and can even take place on board aircraft and maritime vessels situated beyond any national jurisdiction. Clinicians routinely review medical images, and so on, across boundaries. International teams involved in disaster relief can rely upon health information systems in jurisdictions other than their home jurisdiction. The legal, liability and ethical considerations need to be taken into account in the design and deployment of health information systems.

See ISO 13131.

6.8 Information security event reporting

Control 6.8, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Organizations should inform the subject of care whenever unavailability or loss of integrity of health information could have adversely affected their care. Information security events can include patient safety incidents where data processing or information transfer played a role.

Organizations should inform the subject of care whenever personal health information has been inappropriately disclosed. In some jurisdictions, this can be required by law. In many jurisdictions there is a legal requirement to report data breaches involving personally identifiable information to the data subjects whose personal information has been breached.

6.9 HLT – Management training

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive, #Corrective	#Confidentiality, #Integrity #Availability	#Protect, #Respond, #Recover	#Governance, #Legal_and_compliance, #Information_security_assurance	#Governance_and_Ecosystem, #Protection, #Defence, #Resilience

Control

Management of the organization should receive appropriate training, as relevant for their roles and responsibilities with regard to information security and how it is managed.

Purpose

To ensure that management can fulfil its roles and bear its responsibilities with regard to the information security management system.

Guidance

The management of the organization is awarded various roles and responsibilities through this document (and ISO/IEC 27002) and elsewhere. The specific roles and responsibilities should be inventoried. Then, a gap analysis should be performed in order to establish which training is needed.

Since the membership of the organization's management teams can change regularly, the steps above should be repeated as necessary.

Other information

See also 6.3.

7 Physical controls

7.1 Physical security perimeters

Control 7.1, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Many operational areas are permeated by subjects of care. At the same time, the physical safety and security of the public (subjects of care and their support companions), as well as of the data and systems that can be accessible within that environment, should be preserved. For example, a subject of care can be left unattended in an examining room (for example, to allow the subject of care to change into a gown for physical examination), despite the presence of a functioning workstation in the room. Workstation security in healthcare cannot therefore depend entirely upon the exclusion of subjects of care from a security perimeter.

In healthcare, situations can arise where subjects of care (or others) will not always act rationally. This can apply, for example, to young children, people with mental health issues, people who have recently been confronted with distressing news, neurodivergent people, people under the influence of drugs and/or alcohol and so on. Physical security measures should reflect this appropriately.

Consideration should be given to the security of ICT equipment (including mobile phones) belonging to subjects of care while they are unable to provide for security themselves.

Physical security measures for data and systems should be coordinated with more general physical security and safety measures.

7.2 Physical entry

Control 7.2, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

The provision of healthcare includes distinct circumstances where the public (subjects of care and their support companions) are physically admitted into areas where sensitive information is being processed. Physical areas where health information is gathered and/or that contain systems where data are viewed on screen should therefore be subject to additional precautions.

In certain cases, personal health information is displayed on screens and is visible to people who are not entitled to see it. An example is the screen that is presented to a subject of care during the administrative phase of admission and possibly can be read by the next in line. Another example is large informational displays (screens or whiteboards) showing the room or bed allocation on a ward. These displays are intended for use only by clinical and other personnel but can be read by all visitors to the ward. In such cases, information disclosure to unauthorised persons should be prevented, for instance, by changing the location or placement of said displays.

7.3 Securing offices, rooms and facilities

Control 7.3, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.4 Physical security monitoring

Control 7.4, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.5 Protecting against physical and environmental threats

Control 7.5, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.6 Working in secure areas

Control 7.6, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

7.7 Clear desk and clear screen

Control 7.7, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

In cases where the facilities are provided, care should be taken to ensure that timeout and automatic logout features are appropriately configured.

Particular care is needed in certain areas such as operating theatres and intensive care units where it can be necessary to disable timeouts and automatic logouts for safety reasons. In such cases, appropriate procedures should be in place to prevent unauthorized viewing or other activities when use of items of equipment or

devices is definitely not required. However, caution is necessary because devices and equipment can be in use even if unattended or displays are not viewed for prolonged periods.

7.8 Equipment siting and protection

Control 7.8, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

ICT equipment and medical devices incorporating health software can require special security considerations about the environment in which they operate and to the electromagnetic emissions that occur during their operation. Health organizations, especially hospitals, should ensure that siting and protection of such equipment and devices minimises exposure to such emissions.

7.9 Security of assets off-premises

Control 7.9, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Organizations should ensure that any use, outside their premises, of medical devices incorporating health software has been authorized. This includes equipment used by remote workers, even where such usage is for an indefinite period (i.e., where it forms a core feature of the employee's role, such as for ambulance personnel, therapists, etc.), and equipment used by subjects of care.

7.10 Storage media

Control 7.10, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

All personal health information stored on removable media should be encrypted.

Purpose for health (supplementary)

To prevent misuse of personal health information including unauthorized access, disclosure or modification.

Guidance for health

The most commonly recognized types of removable storage media are secure digital (SD) cards and universal serial bus (USB) drives.

Subscriber identity module (SIM) cards are also removable in many cases and often hold confidential information. In addition to mobile phones, devices, including tablets and laptops can incorporate SIMs. SIMs are used in many other circumstances including, for example, remote monitoring systems for building and facilities management, building security alarms, and motor vehicles.

Many items of equipment can include in-built storage including hard drives, solid-state drives (SSDs) and non-volatile memory. However, the presence of such storage is not always documented, evident or expected. Examples include printers (particularly those intended for more than one computer or user and that are networked), stand-alone copiers, and medical devices incorporating health software.

Maintenance, repair and disposal of any equipment containing storage requires additional precautions.

Other information for health

Regarding equipment maintenance see 7.13, regarding secure disposal of re-use of equipment see 7.14 and regarding encryption see 8.24.

7.11 Supporting utilities

Control 7.11, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Electrical power is essential for many aspects of healthcare and loss of power, particularly to certain medical devices, can result in serious harm to subjects of care. For this reason, many hospitals and other healthcare premises have emergency electrical supplies, which continue to provide power (often through specially designated outlets) in the event of a major supply failure, to essential medical or ICT equipment and devices.

Emergency power can be provided in different ways but the quality is not always the same as a normal supply. For example, there can be voltage and frequency fluctuations or other variations. This is also the case when switching (in either direction) between the normal and emergency power supplies takes place. Therefore, even if equipment is protected by connection to an emergency supply, additional measures (such as dedicated uninterruptible power supplies) can be necessary in certain circumstances. There is considerable evidence that, when needed, emergency supplies do not always operate as intended, for example because stand-by generators fail or emergency supplies are overloaded. Therefore, appropriate contingency measures for such events should be considered.

7.12 Cabling security

Control 7.12, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Measures should be taken to prevent unauthorized access through network outlets in publicly accessible and other areas. The following should be considered:

— Disabling ports that are not in use (either physically at patch panels for example or, if available, with suitable network administration tools);

— Disabling any form of access (including traffic monitoring) to devices that have not been previously authorized;

— Use of intrusion detection tools;

— Monitoring unexpected physical disconnection of devices – this may indicate a network cable has been unplugged so that an unauthorized device can be connected instead.

Network outlets are also vulnerable to physical damage. Children and some adults can be destructive, whether accidentally or intentionally. Precautions should be taken to prevent the insertion of objects or substances into outlets by young children, particularly in dedicated wards for them.

Other information for health

See 7.1 for other physical security considerations.

7.13 Equipment maintenance

Control 7.13, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Patient safety should be taken into account both when preparing for and when undertaking all equipment maintenance activities.

Policies should be in place for safe and secure equipment maintenance. A maintenance plan, including both an up-to-date risk assessment and contingency arrangements, should be developed in accordance with the

relevant policies. Before maintenance takes place, the completed plan should be approved in writing by senior management.

In all cases, steps should be taken to ensure that there are no unexpected events, particularly outages (such as loss of network connectivity), that affect systems and devices dependent on the equipment being maintained. Special care is necessary when maintenance is being undertaken remotely or by a third party.

7.14 Secure disposal or re-use of equipment

Control 7.14, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Almost all digital equipment has some form of non-volatile storage, whether or not the equipment has internal (solid-state or hard) disks or ports for removable storage media. This includes medical devices incorporating health software. In addition, non-medical devices such as printers, and network equipment can log or store health or other confidential information (such as network configurations).

Medical devices and equipment can have specific disposal protocols. For example, decontamination as well as other processes can be required to avoid subsequent risk to health. Organizations should ensure that arrangements for disposing of medical devices and equipment include checks for any storage media.

Other information for health

See 7.10 for further information on storage media.

8 Technological controls

8.1 User endpoint devices

Control 8.1, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Other information for health

User endpoint devices can include mobile devices such as smartphones, portable medical devices and wearables.

8.2 Privileged access rights

Control 8.2, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Other information for health

Guidance on privilege management in healthcare can be found in the ISO 22600 series.

8.3 Information access restriction

Control 8.3, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.4 Access to source code

Control 8.4, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.5 Secure authentication

Control 8.5, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Control for health (supplementary)

At least two factor authentication should be used for systems that process personal health information.

Purpose for health (supplementary)

To ensure greater security for access to personal health information.

Guidance for health

Special consideration should be given to the technical measures by which subjects of care are securely authenticated when accessing all or part of their own information (in those health information systems that permit such access).

Consideration should also be given to the ease of use of such measures for subjects of care who have accessibility or other issues. Additional consideration should be given to the subject of care proxies.

8.6 Capacity management

Control 8.6, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

The proportion of medical devices that either can or need to be connected (whether wirelessly or by cable) to a network is increasing rapidly and capacity management should take account of this. Other factors to consider are the potentially high and rising levels of demand both for patient entertainment systems and on guest networks.

8.7 Protection against malware

Control 8.7, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Where installation of software that protects against malware is possible in medical devices incorporating health software, that anti-malware software can interfere with the safe operation of such devices. Software that protects against malware should only be installed or updated in accordance with both the manufacturers' instructions and local policies.

In cases where the use of anti-malware software is not possible, compensating controls, based on a risk assessment, should be implemented as necessary.

8.8 Management of technical vulnerabilities

Control 8.8, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

In large-scale environments, there can be considerable exchange of data both within and between organizations. This exchange can take place across many different interfaces and can be between large numbers of systems and devices, and use a wide range of technologies. Detailed consideration of technical vulnerabilities resulting from these interfaces should be undertaken.

For some medical devices incorporating health software, it is either not possible at all or not appropriate for clinical safety reasons to take measures, such as updating software or applying patches, in the same way as on standard ICT equipment. In cases where it is not possible to update software or apply patches, compensating controls, based on a risk assessment, should be implemented as necessary.

Other information for health

See Annex C for further information.

8.9 Configuration management

Control 8.9, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Configuration of connections

Health IT systems that interoperate with other systems within the organisation and externally in order to enable an interoperable electronic health record are configured initially to conform to the suggested guidance. They must also be maintained in order to continue to enforce the adopted standards as the parameters of their connections change, whether those changes are due to systems changes under the control of the organisation or due to changes external to the organisation.

Configuring medical devices

For patient safety reasons, it is often a legal or local policy requirement that medical devices are configured and maintained by qualified or licensed clinical engineers/scientists.

Many medical devices incorporating health software can exchange information with other devices or health IT systems. Such information exchange can take place through permanent or temporary network connections or by other means such as direct connection. The relevant interfaces are typically the responsibility of ICT professionals who, in some cases, also support operating systems, system utilities, database software and anti-malware software on certain medical devices.

Accordingly, both clinical engineers/scientists and ICT professionals can have responsibilities for (different or overlapping) aspects of the same items of equipment. Configuration management should take account of these issues.

Similar considerations apply to areas other than medical devices. For example, certain items of equipment for delivering medical gases, subjects of care call systems as well as building and facilities management systems are often networked but the responsibility of qualified or licensed engineers. Engineers with such responsibilities are often not clinical engineers/scientists.

8.10 Information deletion

Control 8.10, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Consideration should be given to situations where information is (temporarily) stored on devices that are not managed by the organization. Examples of such situations are “bring your own device" and access to information through personal computers that are privately owned.

Other information for health

See also 7.10 and 7.14 in connection with storage media and circumstances under which information should be deleted.

8.11 Data masking

Control 8.11, the associated attribute table, purpose and other information as given in ISO/IEC 27002 apply.

Guidance for health

The guidance given in ISO/IEC 27002 applies with the exception of b) and c) of the items that "should be considered when implementing data masking techniques". For health, these issues are covered in 5.34 of this document, ISO 27799.

Other information for health

For information on pseudonymization in health see ISO 25237.

8.12 Data leakage prevention

Control 8.12, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.13 Information backup

Control 8.13, 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 backed up in an encrypted format.

Purpose for health (supplementary)

To protect confidentiality of personal health information.

Guidance for health

As a general precaution and specifically to avert ransomware attacks, measures such as storing backup data offline or adopting an immutable backup technology should be considered.

Other information for health

See 8.24 regarding the use of cryptography.

8.14 Redundancy of information processing facilities

Control 8.14, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.15 Logging

Control 8.15, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Other information for health

Guidance on audit trails for electronic health records can be found in ISO 27789:2021.

8.16 Monitoring activities

Control 8.16, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.17 Clock synchronization

Control 8.17, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.18 Use of privileged utility programs

Control 8.18, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

As explained in 8.9, professionals from different disciplines can have (different or overlapping) responsibilities for aspects of particular items of equipment. Policies and procedures for use of privileged utility programs should take account of these issues.

8.19 Installation of software on operational systems

Control 8.19, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

The delivery of care in a healthcare organisation can include hardware devices and software installations that are certified for safe operation with very specific configuration parameters. In certain cases, the certification can prohibit changing any part of the software stack, including making security patches. In such cases, the organisation should record known vulnerabilities in operational systems and the mitigations employed to enable the continued safe operation of those systems.

8.20 Networks security

Control 8.20, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.21 Security of network services

Control 8.21, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

The impact of loss of network service availability of the (clinical) practice should be considered. See also 5.29.

8.22 Segregation of networks

Control 8.22, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Other information for health

Patching, software or firmware upgrades, and the use of software that protects against malware are all techniques that help to maintain security. In some cases (for example, certain medical devices incorporating health software), the use of these techniques is restricted (see Annex C) and compensating controls are necessary. One such control to protect otherwise vulnerable assets is network segregation.

Segregation of patient entertainment systems is often advisable.

Other information for health

See 8.35.

8.23 Web filtering

Control 8.23, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Policies should be in place to avoid incorrect blocking of content that is relevant to healthcare. Such policies should cover handling false positives appropriately.

By default, web filtering systems often block text, images, drawings, videos and other types of content that are entirely appropriate in healthcare but unacceptable in many other contexts. There is a wide range of such content. In addition to anatomical terms and images, examples include content relating to drug use, the results of violence and self-harm, abuse of children and vulnerable adults.

False positives can affect the delivery of healthcare and should be reviewed without undue delay. Correspondingly, there are risks that it is possible to access inappropriate material, under the pretext that it is for legitimate healthcare purposes, and steps should be taken to monitor this.

8.24 Use of cryptography

Control 8.24, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Other information for health

Guidance on policy for issuing and use of digital certificates in healthcare and on the management of keys can be found in ISO 17090-3.

8.25 Secure development life cycle

Control 8.25, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.26 Application security requirements

Control 8.26, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

It is important to consider also personal health information that may not immediately be recognized as PHI, including information about payments or eligibility for healthcare in respect to the individual. Of special concern are circumstances in which personal health information can be derived, such as metadata related to patient communication.

Other information for health

Annex D can be used for the evaluation of security requirements during the development or acquisition of applications.

8.27 Secure system architecture and engineering principles

Control 8.27, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.28 Secure coding

Control 8.28, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.29 Security testing in development and acceptance

Control 8.29, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Acceptance criteria should be established for planned new information systems, upgrades and new versions. Suitable testing of such systems, upgrades and versions should be carried out prior to acceptance.

Acceptance testing of clinically relevant system features should involve clinical users.

8.30 Outsourced development

Control 8.30, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.31 Separation of development, test and production environments

Control 8.31, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Development and testing environments for systems processing health information, as well as training environments, should be separated from production environments hosting those health information systems.

Rules and authorization for the deployment of software from development to production status should be defined, documented and implemented.

Testing should not take place in production environments and should not be performed on personal health information.

8.32 Change management

Control 8.32, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Inappropriate, inadequately tested or incorrect changes to the processing of personal health information can have adverse consequences for the delivery of care and patient safety.

The change process should explicitly record, assess and manage the risks of the change.

8.33 Test information

Control 8.33, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

Guidance for health

Actual personal health information should not be used as test data but steps should be taken to ensure that test data are realistic (see for instance 8.11).

8.34 Protection of information systems during audit testing

Control 8.34, the associated attribute table, purpose, guidance and other information as given in ISO/IEC 27002 apply.

8.35 HLT – Zero trust principles

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Information_protection, #System_and_network_security, #Identity_and_access_management	#Protection, #Defence

Control

Groups of information services, users and information systems that are assigned to a network segment should be kept as small as possible and should only have access to another network segment after both segments involved have authenticated each other.

Purpose

To ensure that entities connected to a network are not trusted by default.

Guidance

Zero-trust security is also known as perimeter-less security. The main concept is "never trust, always verify", which means that information services, users and information systems should not be trusted by default.

Zero-trust is implemented by:

a) establishing strong identity verification,

b) validating device compliance prior to granting access,

c) ensuring least privilege access to only explicitly authorized resources,

d) mutual authentication, including checking the identity and integrity of users and devices without respect to location, and

e) providing access to information systems and information services based on system/device identity and security status in combination with appropriate authentication.

Other information for health

See 8.22.

Annex A
(informative)

Information security controls for health reference

The information security controls listed in Table A.1 are directly derived from and aligned with those listed in Clauses 5 to 8, and can be used in context with ISO/IEC 27001:2022, 6.1.3.

If the control title contains 'HLT', then the control is not included in ISO/IEC 27001:2022, Annex A.

If the control title does not contain 'HLT', then the control is supplementary to the corresponding one in ISO/IEC 27001:2022, Annex A.

Table A.1 — Information security controls for health

5.1	Policies for information security	The information security policy shall 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.
5.2	Information security roles and responsibilities	There shall be at least one individual responsible for information security.
5.9	Inventory of information and other associated assets	All information flows (both within and between organizations) and their interfaces (including integration platforms), shall be included in the inventory.
5.11	Return of assets	There shall 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.
5.12	Classification of information	Personal health information shall be classified as confidential at a minimum.
5.14	Information transfer	Rules, procedures and agreements shall be in place prior to any transfer taking place.
5.15	Access control	Access to personal health information shall be governed by a role-based access control policy.
5.16	Identity management	Users who are to have access to personal health and other confidential information shall be subject to a formal registration process.
5.19	Information security in supplier relationships	The risks associated with access by external parties to systems or the data they contain, shall be assessed and controls that are appropriate to the assessed risk, should be implemented.
5.38	HLT – Information security requirements analysis and specification	The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.
5.39	HLT – Uniquely identifying subjects of care	There shall be policies and procedures to ensure there is a single unique identifier for each subject of care, and functionality to merge duplicate or multiple records in cases where they exist for the same subject of care.
5.40	HLT – Output data validation	When any of an individual's personal health information is displayed or printed, information that safely identifies the subject of care shall be included.
5.41	HLT – Publicly available health information	Publicly available health information shall be protected, traceable, preserved and managed throughout its lifecycle.
5.42	HLT – Emergency communication	Emergency communication within a health organization that functions when ICT continuity has failed, shall be planned, implemented, maintained and tested.

Table A.1 *(continued)*

5.43	HLT – External incident reporting	Information security incidents shall be reported in accordance with legal or contractual obligations.
6.2	Terms and conditions of employment	Job descriptions shall state the security roles and responsibilities that apply to processing of personal health information.
6.6	Confidentiality or non-disclosure agreements	All personnel authorized to access personal health information shall be formally bound to treat such information confidentially.
6.9	HLT – Management training	Management of the organization shall receive appropriate training, as relevant for their roles and responsibilities with regard to information security and how it is managed
7.10	Storage media	All personal health information stored on removable media shall be encrypted.
8.5	Secure authentication	At least two factor authentication shall be used for systems that process personal health information.
8.13	Information backup	Personal health information shall be backed up in an encrypted format.
8.35	HLT – Zero trust principles	Groups of information services, users and information systems that are assigned to a network segment shall be kept as small as possible and shall only have access to another network segment after both segments involved have authenticated each other.

Annex B
(informative)

Correspondence of this document with ISO 27799:2016

The purpose of this annex is to provide backwards compatibility with ISO 27799:2016 for organizations that are currently using that standard and now wish to transition to this edition.

Table B.1 provides the correspondence of the controls for health specified in Clauses 5 to 8 with those in ISO 27799:2016, and should be used in conjunction with ISO/IEC 27002:2022, Annex B.

Table B.1 — Correspondence between HLT-controls for health in this document and in ISO 27799:2016

ISO 27799 control identifier	ISO 27799:2016 control identifier	Control name
5.38	14.1.1	HLT – Information security requirements analysis and specification
5.39	14.1.1.1	HLT – Uniquely identifying subjects of care
5.40	14.1.1.2	HLT – Validation of displayed/printed data
5.41	14.1.3.1	HLT – Publicly available health information
5.42	New	HLT – Emergency communication
5.43	New	HLT – External incident reporting
6.9	New	HLT – Management training
8.35	New	HLT – Zero trust principles

Annex C
(informative)

Information security in health organizations

C.1 Introduction

This Annex provides an outline of certain information security considerations in healthcare. It is intended principally for:

— information security experts including penetration testers and other professionals, such as auditors, with ICT expertise but who are unfamiliar with the health domain;

— medical device, engineering and ICT professionals who work in health organizations and, as such, can have responsibilities for equipment, systems or services that rely on digital technology.

The important subject of the interdependency of security, safety and effectiveness throughout the lifecycle of health software and health IT systems is covered briefly in the Introduction of this document. It is not explored further here but is comprehensively addressed in ISO 81001-1 and related IEC standards.

C.2 Safety of medical devices and equipment

C.2.1 Context

Medical devices and other items of medical equipment that do not perform as intended have the potential to harm patients or other subjects of care.

Depending on the circumstances, harm can be apparent immediately or there can be a delay before harm manifests itself. Some incidents of harm only affect one individual whereas others can affect many people.

In the worst cases, incidents are fatal. However, it can also be devastating for individuals and others, such as family members, when incidents lead to consequences such as irrecoverable and lifelong suffering. In addition, if the results of such harm include the need for 24-hour a day care, the financial consequences are extreme.

In order to minimize the risk of harm, the entire life-cycle of all types of medical device (many of which do not rely on digital technology) and related equipment is heavily standardised and strictly regulated.

C.2.2 Professional responsibility and accountability

Once deployed in health organizations, the safety of all types of medical devices has to be maintained. This is usually the responsibility of professionals such as clinical engineers, clinical scientists, bio engineers or (particularly when ionizing radiation is involved) medical physicists. The precise naming and nature of these roles, as well as the division of responsibilities between them, depends on the devices in question, jurisdictional requirements and local policies. Collectively, however, the individuals performing the roles are termed medical device professionals here.

Similarly, in health organizations, building facilities and building management systems are often the responsibility of engineering professionals, often known as hospital engineers. That term is also used here. In some health organizations, hospital engineers also have responsibility for all medical devices.

In many sectors other than health, professionals in ICT or similar departments typically have responsibility for assets that rely on digital technology and this responsibility can include information security.

However, the responsibilities of medical device professionals and hospital engineers can extend to many aspects of information security. Their departments will normally be provided with instructions, by the manufacturers of assets that depend on digital technology, on relevant information security measures and tasks or activities that need to be undertaken.

Depending on the type of asset, these tasks can include: patch installation, software or firmware upgrades, configuration changes, updating software that protects against malware and so on. The assets typically have to be (taken safely) out of service before such tasks can been undertaken. Afterwards, the assets have to be put back into service. This can involve testing, recalibration or other activities that only the relevant professionals are permitted to undertake.

Many of the assets that are the responsibility of medical device or hospital engineering professionals rely on (cabled or wireless) networking or are accessed from end-user equipment such as PCs, laptops or other mobile devices. In addition, manufacturers of medical devices incorporating health software can require networks and end-user equipment (including apps running on it) to be configured in particular ways to support medical device operation or for information security reasons.

However, the networking and end-user equipment is often the responsibility of ICT professionals. It is therefore possible for information security responsibilities to overlap, and it is essential that all the professional groups coordinate their activities. Such coordination is also essential to ensure, for certain devices and systems, that information security activities are not overlooked on the assumption that another professional group is attending to them.

C.3 Asset ownership and organizational obligations

C.3.1 General

Identification of all assets that use digital technology and that a health organization utilizes or is dependent on is critically important. It is also essential to establish responsibility and accountability for all assets that use digital technology.

Particularly in large health organizations, maintaining inventories can be complicated because of the large number of assets and frequent movement or other changes.

Some factors to be taken into consideration are outlined in following subsections.

C.3.2 ICT and medical devices

C.3.2.1 Asset sources and acquisition

Depending on the nature of the health organization, assets that use digital technology can enter it by various means. Some of these means can be unofficial.

Assets that use digital technology and that are deployed in a health organization can be:

— purchased by it;

— hired, leased or rented by it;

— provided to it as part of a contracted service;

— loaned to it – for example from medical device manufacturers or pharmaceutical companies providing items for direct evaluation or to support clinical trials;

— donated to it – for example by charitable foundations;

— imposed on it;

— developed, built or constructed within it;

— shared.

In addition, some parts or units of health organizations can have considerable autonomy. This can apply to organizations that are geographically dispersed. It can also apply for example, in large health organizations in which (groups of) departments or clinical specialties are authorized to acquire and implement at least some assets that use digital technology without needing approval or oversight from any central or corporate functions in the organization.

C.3.2.2 Asset sharing and other types of organization

A health organization can be associated with other health-related organizations (or departments within them) including:

— medical schools and other bodies that provide education and training to existing and aspiring (i.e. students, trainees and so on) health professionals;

— clinical research units and institutions;

— other academic bodies undertaking clinical, medical or health-related research;

— university departments (such as engineering, physics and computer science) researching or developing one or more of: techniques, devices, equipment and software to improve digital solutions for health and medicine.

Assets that use digital technology and which are owned or under the control of these other organizations are, in some circumstances, shared with the health organization. In some cases, such assets are used exclusively by the health organization.

Correspondingly, some of the health organization's assets that use digital technology can be shared with the other organizations or their departments.

In all these shared situations it is essential that the information security of the assets is maintained and that there is no doubt about which organization retains that responsibility.

C.3.2.3 Other asset flows

Particularly if they need more specialist care elsewhere, subjects of care can be transferred urgently between health organizations. It is possible for some equipment, including medical devices incorporating health software, to be transferred with the subject of care in such circumstances.

In other cases, subjects of care may be provided, temporality or permanently, with medical devices incorporating health software for use when they are no longer on a health organization's premises. This can apply for example to monitoring equipment or implanted devices.

C.3.2.4 Assets owned by the workforce or subjects of care

Depending on their use, some assets owned by members of the workforce or subjects of care need to be included in inventories. This applies, for example, if software licensing rules have to be enforced or it is necessary to be able to remotely wipe equipment.

C.3.3 Building and facilities management systems

Health organizations can operate from a variety of premises. Some premises are owned or under the control of the health organizations that are based in them, but this is not always the case. For instance, health organizations can operate from buildings with multiple purposes (including offices, retail, or both) or share premises, such as outpatient clinics, with other health organizations.

In premises that are not wholly under the control of the health organization, it is important to ensure that necessary information security activities are performed on the facilities and building management systems and to identify which parties are responsible for overseeing or performing them.

This can be complicated particularly in premises where building management has been contracted by an owner or landlord to one or more third parties who can, in turn, subcontract further. Complications can also

arise if the building has been equipped by several different parties such as the owner or landlord, managing agents, tenants or other occupiers.

C.4 People

C.4.1 System and information users

C.4.1.1 General

A number of factors need to be considered in connection with:

— identity management, authentication information and role-based access control;

— development of policies and procedures;

— communication and enforcement of policies and procedures;

— awareness, education and training;

— risk assessment and management.

Some the factors are outlined in following subsections.

C.4.1.2 Health workforce

There are many roles in the health workforce. These include:

— doctors, dentists, pharmacists, nurses, midwives, physiotherapists, paramedics;

— healthcare assistants, technicians, medical secretaries, clinical coders;

— administrative, finance, clerical and support staff;

— volunteers, clergy, charity workers.

Members of the work force in a health organization can be one or more of:

— managers or supervisors;

— full-time or part-time;

— in more than one role (for example as a doctor and, separately, as an academic researcher or educator);

— employed or working in other health organisations (regularly or on an ad-hoc basis).

Examples of the basis on which individuals can be on the workforce include:

— permanent contract;

— short-term or temporary contract;

— secondment or placement;

— locum;

— agency staff (provided by an outside organization);

— bank staff (from a pool within the organization)

— visiting (sometimes for providing a 'second opinion') specialist or advisor.

Before achieving full professional status, individuals can be on the workforce as students, trainees or interns.

Some individuals will only be at work outside standard office hours. To cover for unexpected absences, some individuals can end up working in a different ward or department for just a few shifts or even only one.

While many health care staff work only at fixed locations such as hospitals, a substantial number of clinicians work in the community and provide care to people in their own homes or other accommodation, such as nursing homes and care homes, where they reside.

All these workforce factors have multiple implications, including ensuring that:

— personal health information of individuals is only available to those members of the workforce who have a legitimate need to access it; and

— access rights to systems are correctly managed.

Some compromises can be necessary in order to avoid unmanageably complex approaches.

ISO 21398 considers some of these factors further and also provides lists of regulated professional roles in health.

C.4.1.3 Subjects of care and their proxies

Subjects of care (and their proxies) can be given access to their personal health information. In some cases, users have direct access to health information systems but, in other instances, their personal health information is accessed through an app.

Issues to be considered include:

— ensuring that information retrieved or downloaded remains secure on the device used;

— implications of providing users with the ability to update their personal health information not only by direct entry of information but also upload from:

  — health, well-being or fitness devices (that can belong to the health organization or the user) or apps;

  — records from other health organizations where the subject of care has been treated;

— subjects of care who: are children, have accessibility issues or have learning difficulties;

— any restrictions on the information in their own records that subjects of care allowed to see;

— restrictions that subjects of care wish to place on what any proxies they have can access and how these restrictions are managed;

— how the authorization of proxies as users is managed and the extent to which, or not, this can be controlled by the subjects of care.

C.4.1.4 Other users

Examples of other users who can need or be entitled to access personal health or other confidential information, as well as systems holding such information, include personnel from regulatory and inspection bodies, insurers, financial and other auditors, health professionals and others investigating clinical or other incidents. To investigate crime, police and other law enforcement organizations can also be given access to personal health information.

Even if these other types of users claim otherwise, it is not always appropriate for them to be granted unrestricted access to information about particular subjects of care or other individuals (such as members of the workforce).

C.4.2 Information security advisory group

C.4.2.1 Aims

Because information security has such widespread implications for a health organization, it can be beneficial for it to have an information security advisory group (such a group can also be called, for instance, a board, committee or forum).

Aims of the group can include:

— ensuring that there is clear direction and visible management support for ensuring information security;

— keeping users up-to-date about information security issues which they need to be aware of (such as new phishing techniques or malware threats);

— learning lessons from information security incidents and near misses both within the organization and elsewhere;

— coordinating awareness raising, education and training for the workforce – this should be not only for new joiners but also as a refresher for others;

— consulting on proposed changes as these can affect clinical practice, business processes or both; for example, shortening session inactivity timeouts or resetting large numbers of passwords can have unintended consequences such as preventing or delaying access to systems in clinical emergencies, or causing interfaces to fail.

C.4.2.2 Membership

There should always be representation on the group from top level management and the organization's information security experts. Stakeholders who can be represented depend on the type and size of health of organization. They can include:

— clinicians and other members of the workforce closely involved in the direct care of patients;

— academic, teaching and research staff;

— other non-clinical staff who use different systems, typically from departments such as: finance, human resources, procurement/supplies, press and communications.

Clinical and business processes, as well as systems used, can vary substantially between clinical specialties. Accordingly, to give a more balanced view in large organizations, it helps to have attendees from several clinical specialties on the group. It can also be helpful to have some junior staff, trainees or students involved in the group. This is because their experiences, as well as their exposure to different information and systems, can vary considerably from those of senior staff or management.

C.4.3 Technical roles and coordination

As previously noted, medical device, hospital engineering and ICT professionals can have responsibility for various aspects of information security and therefore need to coordinate their activities.

However, there can be individuals in other groups or professions who have technical information security responsibilities such as installing patches and updating software. These individuals are typically system managers or system administrators of specialist clinical or departmental systems. As such their day-to-day duties can include authorizing users of the systems, running backups and so on. Examples:

— Pathology laboratory analysers and related equipment can be supplied with a laboratory information system. Such systems will typically export results through interfaces and it is only laboratory staff who access the systems directly. The system manager is usually a member of the relevant department and could be a pathologist or a laboratory manager.

— An individual in a department that ensures physical security in a hospital can be responsible for systems such as those for identity cards and security passes, door entry systems, intrusion alarms and surveillance.

It is therefore important for there to be coordination between departmental system managers, or others who can perform technical information security tasks, and the organization's overall information security professionals.

Another area, affecting ICT and hospital engineering departments, in which there can be overlapping responsibilities or, conversely, (usually inadvertent) gaps in coverage is the building infrastructure that supports ICT. This infrastructure includes network cabling, patch panels, network outlets, communications and computer rooms, and uninterruptible power supplies.

C.5 Asset types and uses

C.5.1 General

The following sub-sections provide examples of various types of asset that use digital technology. Because of the very wide range of such assets, the examples cannot be comprehensive. The purpose of the examples is to provide outline checklists and to highlight that a rigorous approach is needed to avoid omission of any assets from inventories.

C.5.2 ICT and IoT

C.5.2.1 Generic equipment and services

As in many other sectors, much generic ICT and, increasingly, IoT (Internet of Things) technology is used in health.

One area of note is patient entertainment systems which provide TV and streaming services to the bedside. These systems can routinely place very large loads, which exceed all other traffic combined, on hospital networks. In addition, demands on these systems can peak dramatically if large numbers of users all want to access the same broadcast at the same time; this can happens when there are high-profile news or sporting events.

C.5.3 Medical devices

Medical devices can be classified or categorized in many different ways. The grouping and order of the medical devices incorporating health software in the list that follows are of no particular significance.

— implantable devices such as pacemakers and defibrillators;

— imaging equipment: Digital Radiography (DR) and other x-ray based devices, CT (Computed Tomography) scanners, MRI scanners, ultrasound scanners, endoscopy equipment;

— anaesthetic machines;

— haemodialysis machines;

— radiotherapy equipment;

— surgical robots;

— ventilators;

— external defibrillators;

— laboratory analysers;

— infusion pumps, syringe drivers;

— point of care testing devices;

— monitoring and diagnostic devices including those for: temperature, heart rate, respiratory rate, blood pressure, oxygen saturation, blood glucose level, electrocardiography, electroencephalography.

Many of the devices listed are normally only found in premises or locations (such as hospitals, clinics, diagnostic centres, hospices and nursing homes) that are specifically for health care. However some medical devices incorporating health software can also be found in mobile trailer units (this applies particularly to certain types imaging equipment) and ships. Ambulances and other means of transport (such as helicopters) used by emergency services also use certain medical devices incorporating health software.

C.5.4 Building and facilities management

C.5.4.1 Generic equipment and services

Premises in which health services are delivered typically have systems, plant and machinery which are deployed in many types of buildings and are generic. These generic items provide, for example:

— HVAC (heating, ventilation, and air conditioning) and environmental controls;

— fire detection and suppression;

— lighting control including for example occupancy sensing;

— energy management;

— electronic signage and public address facilities.

C.5.4.2 Physical security systems

There can be generic security systems in health premises such as:

— access control and door entry systems;

— surveillance systems including security cameras;

— intrusion detection and alarm systems;

— personal alarms and body-worn cameras for members of the workforce.

C.5.4.3 Health-specific equipment

Health-specific items of equipment (some of which are classed as medical devices) and related systems specific to health buildings include:

— medical gases and vacuum including monitors and alarms;

— refrigeration and temperature-controlled storage (of blood products, drugs, pathology samples, and so on);

— permanently installed sterilizers (also known as autoclaves);

— nurse call and similar alerting systems as well as other bedhead services.

C.5.5 Uses of personal health information

C.5.5.1 General

Reviewing all the ways in which personal health information is being used or processed in a health organization can assist in both identifying assets that use digital technology and confirming completeness of inventories.

C.5.5.2 Classification of purposes for processing personal health information

ISO/TS 14265 provides a detailed classification of purposes for processing personal health information. The main entries at the topmost level of the classification are as follows:

a) person centred care - processing that directly or indirectly contributes to the health and care of an individual;

b) health service management and quality assurance - processing that utilises the personal data of an individual in order to monitor and improve the quality, safety and equity of health and care provision to a broad range of individuals;

c) population and public health - processing personal health data to track public health concerns, manage public health risks to individuals and populations, and develop effective strategies;

d) clinical research- the design and conduct of clinical trials, real world data studies and other forms of knowledge generation that involve the processing of personal health data;

e) education and training - processing personal health data to develop education and training materials, to deliver teaching or to evaluate learning;

f) compliance with legal obligations - disclosing or processing personal data in compliance with laws or judicial instructions.

C.5.5.3 Record Lifecycle Events

In addition to considering overall purposes for processing personal health information, possible actions on records can be reviewed in order to identify assets that use digital technology and confirm completeness of inventories.

ISO 21089 specifies the following set of Record Lifecycle Events: access/view, add legal hold, amend (update), archive, attest, decrypt, de-identify (anononymize), deprecate, destroy/delete, disclose, encrypt, extract, link, merge, originate/retain, pseudonymize, re-activate, receive/retain, re-identify, remove legal hold, report (output), restore, transform/translate, transmit, unlink, unmerge, verify.

These events are also those that ISO 27789 specifies for inclusion in audit logs.

C.5.6 Health and other applications

C.5.6.1 Health organizations

Hospitals and other premises where health services are provided can have a range of health IT systems (the names of which can vary) principally for direct care purposes including:

— electronic patient record (EPR) systems;

— patient administration systems (PAS);

— picture archiving and communication systems (PACS);

— laboratory information management systems;

— radiology information system (RIS);

— pharmacy/dispensing systems;

— clinical systems for particular specialties (of which there can be plenty in large organisations) such as maternity, cardiology or ophthalmology;

— departmental systems for example: theatres, sterile supplies or infection control;

— interface engines.

These systems can provide a variety of functions including: holding health records, clinical decision support, and scheduling and booking of: appointments, consultations and operations.

As can be inferred from the classification of purposes in ISO/TS 14265, there can be many other systems processing personal health information. There can also be document and content management systems, websites, intranets and so on as well as systems for: administrative, financial, workforce rostering, education and training (including learning management systems and virtual learning environments), retail (such as for staff and visitor refreshments) and other purposes.

The key point is that, depending on the organization, there can be an unexpectedly large number of systems and databases, many of which contain personal health or other confidential information. In large teaching hospitals in particular, the evidence is that there can be hundreds.

For the future, significant increases in the use of systems that use artificial intelligence (AI), genomic information, or both are inevitable.

C.5.6.2 Asset and personnel tracking

Asset tracking and motoring systems using RFID (radio-frequency identification) tags, bar codes or other technologies can be used for many purposes including locating medical devices, when dispensing drugs, and managing stocks of consumables, blood products or surgical instruments. The use of bar codes for pathology samples is very common.

Certain health organizations track the locations of some of their workforce. This can be for various reasons including, for example, business process analysis and improvement. Clinicians who work in the community can be tracked for their physical safety.

Hospital inpatients usually have identity bands. These can have barcodes. Some health organizations use tracking technology for certain subjects of care. Examples include:

— individuals who can become lost or disoriented because they suffer from dementia or other conditions;

— new-born babies (if they are moved from designated areas, alarms are sounded to prevent abductions).

C.5.6.3 Apps

Health, well-being and fitness apps are increasingly common. Some are developed specifically for use with other products such as portable medical devices, fitness monitors, wearables and so on.

Some health organizations develop or license apps for subjects of care or their workforce. However many health-related apps are sourced (usually from 'app stores') in the same way as apps of any other type.

Some health-related apps can be beneficial. However, many health-related apps are associated with safety, privacy or security risks, frequently in combination.

C.5.7 Interfaces

Information on subjects of care is often captured or stored in interconnected health IT systems (that can consist of medical devices incorporating health software, middleware, multiple databases, and so on). Much of this information has to be shared or exchanged for care or other purposes; interfaces are commonly used to transfer the relevant data.

Interfaces both within and between organizations can present many different types of security and privacy risks. As such it is essential that they are all included in asset inventories.

Some interfaces use proprietary protocols and data formats. However the heterogeneous nature of health IT systems and medical devices incorporating health software is such that interfaces, particularly between different manufacturers' products, often exploit standards for exchanging health information.

The most commonly specified and used standards for exchanging health information are as follows:

— HL7 Version 2.5 as specified in ISO/HL7 27931;

— HL7 FHIR (Fast Healthcare Interoperability Resources);

— DICOM (Digital Imaging and Communication in Medicine) as specified in ISO 12052;

— ISO/IEEE 11073 series.

Profiles of DICOM and HL7 standards developed by IHE (Integrating the Healthcare Enterprise) are also common

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

D.1 Purpose

This informative annex provides example security and privacy requirements that can:

— Inform the procurement, enhancement and evaluation of health software products and information systems from a security and privacy perspective;

— Assist organizations implementing ISO 27799 controls and guidance in shaping information privacy and security policies, regulations, guidelines, protocols and procedures;

— Foster implementation of security controls in the health IT system lifecycle.

The organization using this annex as the basis for its own evaluation can modify the suggested requirements as needed for the specific circumstances of the organization's process. In addition, Annex D presents the relationships between these example security and privacy requirements for health information systems derived from the withdrawn ISO 14441:2013 and the ISO 27799 controls. A mapping to the security capabilities identified in IEC TS 81001-2-2:202x Guidance for the implementation, disclosure and communication of security needs, risks and controls is also included. IEC TS 81001-2-2:202x presents an informative set of common, high-level security-related capabilities and additional considerations to be used across the entire life cycle of health software (including medical device software) and for the information exchange between the medical device manufacturers, health software manufacturers, health delivery organizations and/or other stakeholders as presented in Table D.1 below.

Table D.1 — Security Capabilities described in Clause 5 of IEC TS 81001-2-2:202x

Section	Capability	Acronym
5.2	Automatic logoff	ALOF
5.3	Audit controls	AUDT
5.4	Authorization	AUTH
5.5	Cybersecurity product upgrades	CSUP
5.6	Health data de-identification	DIDT
5.7	Data backup and disaster recovery	DTBK
5.8	Emergency access	EMRG
5.9	Health data integrity and authenticity	IGAU
5.10	Malware detection / protection	MLDP
5.11	Node authentication	NAUT
5.12	Person authentication	PAUT
5.13	Physical locks on product	PLOK
5.14	Third-party components in product life cycle roadmaps	RDMP
5.15	System and application hardening	SAHD

Table D.1 *(continued)*

Section	Capability	Acronym
5.16	Health data storage confidentiality	STCF
5.17	Transmission confidentiality	TXCF
5.18	Transmission integrity	TXIG

D.2 Audience

The target audience for this informative annex includes organizations and individuals that:

— are involved in supply, procurement, configuration, integration and implementation of health software and health IT systems;

— are responsible for planning, adoption and testing of health IT systems, from privacy and security perspectives.

D.3 Mapping tables

The relationships between the example security and privacy requirements and the ISO 27799 controls are many-to-many. To simplify the use of the mapping, the relationships have been represented in two tables, each of which represents a set of one-to-many relationships:

— Table D.2: Relationships between the security and privacy requirements and the ISO 27799 controls. It has three columns:

  — Left column – Security and privacy requirements

  — Middle column – Applicable security capabilities from IEC TS 81001-2-2:202x

  — Right column – ISO 27799 Controls

— Table D.3: Relationships between the ISO 27799 controls and the security and privacy requirements. It presents two columns, in reverse order from the first table:

  — Left column – ISO 27799 Controls

  — Right column – Security and privacy requirements

The middle column in Table D.2 presents an additional mapping to the security capabilities presented in IEC TS 81001-2-2:202x. Manufacturers should also see the informative annex of IEC TS 81001-2-2, Annex A, Sample scenario showing the exchange of security information, and Annex A, Section A.2, Manufacturer Disclosure Statement for Medical Device Security (MDS2), for an example of how a medical device manufacturer might benefit from this mapping.

Table D.2 — Relationships between the security and privacy requirements, the security capabilities in Clause 5 of IEC TS 81001-2-2:2024, and the ISO 27799 controls.

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
Data subject's consent to collect, use or disclose personal health information		

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
R1 Recording consent: where data subjects have a right, by law or custom, to withhold or revoke their consent to collect, use or disclosure of their personal health information, health information systems: a) shall provide a facility to record a data subject's consent directives, including the withholding or revocation of consent; b) shall be able to accomplish this in a way that allows each organization to comply with its own legal or policy requirements on consent; **R2 Minimum data recorded:** where health information systems record a data subject's consent directives, the characteristics of the directive shall be recorded (for example, the withholding of consent, or the withdrawal of consent previously given) as well as the type of consent in those jurisdictions that recognize two or more types of consent (for example, implied consent versus expressed consent) and the date on which the directive was given. **R3 Directives follow the data:** where data subjects have a right, by law or custom, to withhold or revoke their consent to the collection, use or disclosure of their personal health information, health information systems should provide a facility to transmit restrictions on further (i.e. onward) disclosure along with the data disclosed if the recipient(s) of the disclosure could not otherwise be aware of and honour the data subject's consent directives. The health information system should be able to accomplish this in a way that allows the sending and receiving jurisdictions to comply with their own legal requirements or policies on consent.	AUDT AUTH DIDT EMRG IGAU NAUT PAUT STCF TXCF TXIG	5.1 Policies for information security 5.2 Information security roles & responsibilities 5.15 Access control 5.20 Addressing information security within supplier agreements 5.24 Privacy and protection of PII 5.33 Protection of records 5.34 Privacy and protection of PII 8.15 Logging 8.16 Monitoring activities
R4 Emergency access: emergency medical care (such as that given to an unconscious subject of care) or other special situations permitted by law or policy (such as public health investigations during communicable disease outbreaks) may necessitate access to patient records stored in a health information system with partial compliance allowed by law or policy with previously recorded consent directives. Such emergency access capability shall only be provided to authorized users and its invocation (along with a reason the user is overriding the consent directive) shall be recorded in an audit log. Except where partial overriding of consent directives is allowed by law or policy, and to eliminate uncertainty as to whether a user intended to override subject of care consent directives, the system should either allow the user to expressly invoke emergency access or else the system should inform the accessing user, prior to granting access, that the access will constitute emergency access. **R5 Logging emergency access:** health information systems shall be able to: a) log when the processing of consent directives prohibits the disclosure of data; b) log the identity of any user who overrides a data subject's consent directives, the reason for the emergency access, a unique identifier that can be later used to identify the data subject, the date and time when the emergency access occurred; c) provide notification of emergency access to individuals accountable for facilitating privacy compliance.		

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
R6 Consent given by a legally authorized representative: where a consent directive is given on behalf of a subject of care by a legally authorized representative, the health information systems should be able to record the identity of this representative and the representative's relationship to the subject of care. **R7 Reporting changes to consent**: for any given subject of care, health information systems recording consent directives shall be able to indicate which consent directives, if any, were in force at any given point in time and when any changes were made.		
Limiting use and disclosure		
R8 Recording and storing only that data which have an identified purpose for its collection, use or disclosure: personal health information should only be used or disclosed for purposes consistent with those for which it was collected. **R9 Limiting disclosure of data subject's information to healthcare providers with a relationship to the data subject**: it should be recorded (for example, the withholding of consent, or the withdrawal of consent previously given) as well as the nature of consent in those jurisdictions that recognize two or more types of consent (for example, implied consent versus express consent) and the date on which the directive was given. **R10 Restricting data exports**: data transmission in electronic or printed format between health information systems should only be permitted for identified purposes such as clinical care, data backup, or transmission to the data subject (or the data subject's agent) at the subject's request.	AUDT AUTH DIDT EMRG NAUT PAUT STCF TXCF TXIG	5.1 Policy for information security 5.12 Classification of information 5.13 Labelling of information 5.15 Access control 5.20 Addressing information security within supplier agreements 5.33 Protection of records 5.39 Uniquely identifying subjects of care
Data subject access to personal health information & correction of information		
R11 Data subject access: when a data subject challenges the completeness or accuracy of information in the subject's record, and the organization disagrees with the subject's assessment of incompleteness or inaccuracy, the health information system should be capable of recording the disagreement and/or the reason for the refusal to update the record. **R12 Accessibility**: health information systems should be capable of output or display of personal health information in formats that can be read by the subjects of care, including persons with disabilities, impairments or sensory loss	IGAU STCF	5.12 Classification of information 5.13 Labelling of information
Data Accuracy		
R13 Accuracy: health information systems shall include measures to ensure that personal health information is accurate and complete as is necessary for the purposes for which it is to be used. Examples include implementing data input validation controls and using integrity checks such as checksums and hash totals. **R14 Subject of care identification**: health information systems shall accurately identify a subject of care in the system by means of unique identifiers, searchable by users, when accessing or modifying the subject's records.	AUDT IGAU STCF TXCF TXIG	5.39 HLT - Uniquely identifying subjects of care 5.40 HLT - Output data validation
User identification and authentication		

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
R15 User identification: users of health information systems shall be assigned an identifier (user ID) that, perhaps in combination with other identifiers (e.g. facility identifiers, jurisdictional identifiers) if necessary, uniquely identifies each individual user and that is used in user authentication and audit logging. Where transactions extend across organizational or jurisdictional boundaries, user IDs, in combination with other user registration information (e.g. user names, addresses, facility identifiers, jurisdictional identifiers) shall: a) uniquely identify each user, b) allow access control decisions, and c) allow the compilation of audit records that can unambiguously associate user identities with their audited user actions. **R16 User IDs**: health information systems shall support case-insensitive user identifiers that contain characters drawn from ISO/IEC 8859 (all parts) (e.g. ISO/IEC 8859-1, also known as US ASCII) or from ISO/IEC 10646 (also known as Unicode). **R17 Secure authentication**: health information systems shall authenticate the identity of every entity (e.g., users, applications, system services) seeking access to personal health information before granting them access to data and systems resources. **R18 User authentication**: health information systems shall authenticate every user before access to personal health information or related health information system services are granted to the user. For greater clarity, this includes access granted when not connected to a network (e.g. when the health information system is available for access offline). **R19 Authentication methods**: health information systems should support multi-factor user authentication. **R20 System authentication**: health information systems shall authenticate every system entity seeking access to personal health information. Health information systems shall ensure the authenticity of remote nodes (mutual node authentication) when communicating personal health information over the Internet or other known open networks by using a secure standards-based protocol. **R21 Protecting user profiles, passwords, and other authentication tokens**: all data or parameters used in the health information system user authentication process shall be stored or transported in a secure manner and protected from unauthorized access (including viewing, modification, or deletion). Where user passwords are employed, either implement secure password salting and hashing methods or encrypt the passwords using cryptographically secure algorithms. **R22 Passwords**: **use, quality, reset, and user changes**: when passwords are used, the health information system shall implement the following:	ALOF AUDT AUTH EMRG NAUT PAUT	5.16 Identity management 5.17 Authentication information 5.18 Access rights 5.38 Information security requirements analysis and specification 6.7 Remote working 8.1 User endpoint devices 8.2 Privileged access rights 8.3 Information access restriction 8.4 Access to source code 8.5 Secure authentication 8.11 Data masking 8.12 Data leakage prevention 8.15 Logging 8.16 Monitoring activities 8.24 Use of cryptography

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
a) password strength: check password strength at the time the user sets it by ensuring, for example, that passwords are composed of a combination of a sufficient number of uppercase and lowercase letters, numbers, special characters, they do not include any users' personal information e.g., a phone number, and do not contain any consecutive letters or numbers, b) frequency of password changes: implement a function that requires users to change their password according to an adjustable maximum time period, c) password history policy: implement an administrative function that prevents users from reusing the same password a certain number of iterations e.g., the last 10 passwords, d) password reset: after a password reset, users shall be required to set a new password at their next successful logon, e) case sensitivity: support case-sensitive passwords that contain characters drawn from ISO/IEC 8859 (all parts) (e.g. ISO/IEC 8859-1, also known as US ASCII) or from ISO/IEC 10646 (also known as Unicode). **R23 Failed Login Attempts**: health information systems shall enforce a limit of consecutive invalid access attempts by a user to protect against further (possibly malicious) user authentication attempts. Examples of appropriate mechanisms include locking the account/node until released by an administrator, locking the account/node for a configurable time period, or delaying the next login prompt according to a configurable delay algorithm. **R24 User feedback during authentication**: health information system shall provide only limited feedback information to the user during authentication that does not assist the user in discovering user IDs and passwords.		
Access control		
R25 Access controls: health information systems shall verify that every authenticated person or entity seeking access to personal health information is authorized to access such information. **R26 Authorization control**: prior to carrying out a system of data function related to personal health information, health information systems shall verify that the requesting user or entity has the required access privileges. **R27 Role-based access control**: health information systems shall support role-based access control (RBAC) capable of mapping each user to one or more roles, and each role to one or more system functions or access privileges.	AUDT AUTH EMRG NAUT PAUT PLOK STCF	5.2 Information security roles & responsibilities 5.15 Access control 5.18 Access rights 5.22 Monitoring, review and change management of supplier services 5.33 Protection of records 5.34 Privacy and protection of PII 6.7 Remote working 7.14 Secure disposal or re-use of equipment 8.3 Information access restriction

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
R28 Other forms of access control: health information systems should additionally be capable mapping each user to access rights assigned or restricted based on: a) working groups to which the user belongs, or b) the context of the transaction (for example, time-of-day, workstation-location, or emergency access). **R29 Delegation of access to the personal health information of subjects of care**: health information systems should be capable of maintaining an association between selected users and the records of subjects of care and permit access based on this association. Health information systems should be capable of granting delegated access to records based upon a user with authorized access to a subject of care's records granting access rights for those records to another user. Where implemented, such granting of access shall not: a) allow a user, by system means, to grant another user access to a record if the granting user does not possess such access with respect to the record, or b) exceed the role-based access privileges of the user being granted the access. **R30 Reporting access privileges**: health information systems shall be able to report, for a given user, whether the user can access the records of a given subject of care and the privileges (viewing, modification, etc.) the user has in respect of the subject's records. **R31 Restrictions on access privileges**: where a user has been assigned more than one user role, the health information system shall allow the user to select which of the roles allocated to the user is to be applied to that user's session. **R32 Revoking access privileges**: health information systems shall support revocation of all a user's access privileges without requiring the deletion of the user account from the system. Health information systems shall prevent users whose access privileges have all been revoked from logging into the system e.g. through changing the user account to inactive		
Acceptable Use		
R33 Notifications to users: in each user's session, either prior or immediately following user login or other periodic intervals, the health information system should display a configurable warning or login banner to remind the user of the confidentiality and appropriate use of the personal health information accessible from the system and/or applicable penalties for misuse of the system.	AUTH EMRG PAUT	5.10 Acceptable use of information and other associated assets
Security and timeout		

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
R34 Workstation timeout: while a particular user's session is active at an unattended workstation, the health information system shall prevent unauthorized access by automatic time-out after a configurable period of inactivity. Examples of such protection include implementation of a screen saver or a screen timeout requiring a legitimate user to re-authenticate. **R35 Application session timeout**: health information systems shall prevent idle application sessions from being accessed by unauthorized person(s) by means of an automatic application timeout after a configurable period of user inactivity. Examples of such protection include implementation of application locking, requiring a legitimate user to re-authenticate. Application timeout should be preceded by a warning (at a configurable interval of time) that timeout is about to take place. When an application session has timed out, the same user should be able to return to the session by re-authenticating, or another user should be able to end the previous session (without reactivating it) in order to be able to proceed with a new session. **R36 Connection timeout**: Health information systems should have facilities to restrict connection durations where required to a configurable period of time and to force a reconnect when the periods have been exceeded. **R37 Session security**: health information system shall have communication session security controls to prevent the user's session from being hijacked or stolen.	ALOF AUDT AUTH EMRG MLDP NAUT PAUT PLOK SAHD TXCF TXIG	8.1 User endpoint devices 8.5 Secure authentication 8.27 Secure system architecture and engineering principles
Maintaining data availability		
R38 Backup: health information system shall support the generation of backup copies of the application data, security credentials, audit log files, as well as other data and files needed for the proper functioning of the health information system. **R39 Concurrent backup**: if the health information system is available continuously, then the system shall have ability to run a backup concurrently with the operation of the application. **R40 Restoration**: health information system data restoration shall enable a user to return the system to a fully operational and secure state. This state shall include the restoration of the application data, security credentials, and audit files, and shall also enable validation of the integrity of the data restored. **R41 Reconstructing the content of an electronic health record at a prior point in time**: health information systems shall have the capability of displaying the content any data subject's record(s) as the recorded existed at any previous date or time.	AUDT DTBK IGAU	5.1 Policies for information security 5.30 ICT readiness for business continuity 8.13 Information backup 8.14 Redundancy of information processing facilities 8.15 Logging 8.16 Monitoring activities
Protecting data during transmission		
R42 Encrypting data during transmission: in a health information system consisting of components distributed across multiple computers or systems, the communication between those components should, (and over the Internet or other open network, shall) offer the following security components: a) partner authentication (e.g. client and server), b) data integrity, and c) data confidentiality. **R43 Confirmation of data delivery**: In order to ensure that transmitted data are received, clinical systems shall implement security controls to confirm delivery or receipt of data when data communications take place outside the physical security perimeter that protects information processing facilities.	AUDT AUTH IGAU NAUT PAUT TXCF TXIG	5.14 Information transfer 5.19 Information security in supplier relationships 8.12 Data leakage prevention 8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks 8.24 Use of cryptography

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
Protecting data in storage		
R44 Protecting operational data: health information systems shall ensure that personal information, audit logs, and security-related data such as user profiles, are all protected from unauthorized access and modification when stored permanently (e.g., within databases or file systems) or temporarily (e.g., cached memory). **R45 Protecting data on portable or removable devices**: when storing personal health information on any media or device intended to be portable or removable (for example, flash drives, optical media, or notebook computer), health information systems shall use of an industry standard encryption format. **R46 Protecting data in data repositories**: health information systems storing confidential and sensitive data including personal health information and security critical system data (e.g., user profile data and audit logs) shall protect these data from unauthorized access.	AUDT AUTH EMRG MLDP NAUT PAUT PLOK SAHD STCF TXCF TXIG	7.10 Storage media 7.14 Secure disposal or re-use of equipment 8.1 User endpoint devices 8.11 Data masking 8.12 Data leakage prevention 8.15 Logging 8.16 Monitoring activities 8.33 Test information 8.34 Protection of information systems during audit testing
Data integrity		
R47 Integrity of data inputs: data imported from anywhere (e.g., a health information system, a medical device, or portable device) shall be accurately associated with a subject of care and a physician in charge, location, date and time of import, and user who imported the data. The health information system used to import the data shall display a warning regarding potential risks. **R48 Integrity of data during processing**: controls shall be in place within the health information system to ensure the integrity of data to prevent user actions or system faults from causing data inconsistencies or integrity failures. **R49 Integrity of data outputs**: health information systems shall ensure it is possible for a reader to check that hardcopy print-outs are complete.	DIDT IGAU TXIG	5.38 HLT – Information security requirements analysis and specification 5.39 HLT – Uniquely identifying subjects of care 5.40 HLT – Output data validation 5.41 HLT – Publicly available health information
Record retention		
R50 Retention: health information systems shall be capable of storing data for configurable retention periods and support retention scheduling methods and procedures to manage different types of data as defined by law or organizational policy. When data are no longer needed, it shall be disposed using secure disposal methods, for example, erasing, cryptographic erasing, media reformatting, or rendering anonymous.	AUDT DIDT DTBK IGAU PLOK STCF	8.10 Information deletion
Data Labelling		
R51 Labelling: health information systems shall be capable of informing each user of the confidential nature of personal health information they access. Examples include displaying the confidentiality label in a consistent location and manner upon user logging into the system, or when displaying personal health information.	IGAU STCF	5.12 Classification of information 5.13 Labelling of information
System and Audit Logs		

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
R52 System logs: health information systems shall support recording of system events and actions e.g., system startup and shutdown, user activity, system performance, system resource usage, and system errors and warnings. **R53 Information recorded**: for each of these events, control information shall be recorded, e.g., time of event, identity and the role of the user (in those cases where a user can choose among multiple roles before commencing a user session). **R54 Protecting the audit log**: the audit log files shall have appropriate security controls to prevent alteration and unauthorized access. Examples of such controls include access controls, continuous monitoring to detect any unusual activities or breaches, encryption, and periodic or continuous backup of log files. **R55 Audit interface**: access to audit data shall be strictly controlled and itself subject to audit. Access should be by an appropriate information system that can enforce these controls, rather than directly to the audit trail itself. The audit system shall provide the capability and investigative tools to read audit information from the audit records and interrogate the audit log to: a) identify all users who have accessed or modified a given data subject's records over a given period of time, or b) identify the actions of a given user (including all access to data subjects' records) over a given period of time. **R56 Audit log retention**: although the duration of retention of audit log files is a matter of organizational policy that may vary from one jurisdiction to another, the audit system shall support retention of audit log entries. **R57 Application audit logs:** health information system shall record events and actions within the system including details regarding: a) subject of care records created or accessed (e.g. displayed on-screen, printed, downloaded) or updated b) accesses data that is locked or masked by instruction of a subject of care/person (emergency access), c) creation and modification in the consent directives of a subject of care/person, d) data queries of personal health information, e) personal health information import (reception) including data transmission, data exchange, f) personal health information export, including data transmission, data exchange and printing, g) user, role, and group management activities, and h) access to audit log. Health information system audit logs should also be capable of capturing the following events:	AUDT SAHD	8.15 Logging 8.16 Monitoring activities 8.33 Test information 8.34 Protection of information systems during audit testing

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
— system start and stop, — user authentication attempts and its result (successful or not), — user logout, session timeout, account lockout, — backup and restore (where initiated by the system itself), — database accesses, — node-authentication failure, — digital signature created/validated, — security administration events, including password changes, and — record disposal. Health information systems should allow an authorized administrator to set the inclusion or exclusion of auditable events not included in the list above. **R58 Minimum content of information recorded**: health information system audit log entries shall include the following information: a) a record of the user identity, b) a record of the identity of the authority – the person authorizing the entry of, or access to data, if different from the user, c) the role the user is exercising (in those cases where a user can choose among multiple roles before commencing a user session), d) the organization of the accessing user (in those cases where a user accesses information on behalf of more than one organization), e) the nature of the audited event and the identity of the associated data (e.g. subject of care's ID, message ID) of the audited event, f) the function performed by the user, g) a time stamp (data and time of the event), h) in the case of emergency access to blocked or masked records or portions of records, a reason for the emergency access, as chosen by the user making the access,		

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
i) in the case of changes to consent directives made by a substitute decision-maker, the identity of the decision-maker, j) end user device or access point (if available), k) In the case of password change, user whose password was changed, and l) a sequence number to protect against malicious attempts to subvert the audit trail by, for example, altering the system date. **R59 Audit interface**: the health information system should support logging to a common audit engine (for example, using the schema and transports specified in the Audit Log specification of IHE Audit Trails and Node Authentication (ATNA) Profile). The system shall provide authorized administrators with the capability to read audit information from the audit records in at least one of the following ways: a) the system should provide the capability to generate reports based on date and time ranges, or b) the system should be able to export logs in such a manner as to allow correlation based on date and time (e.g. UTC synchronization). **R60 Protecting the Audit Logs**: health information systems shall: a) prohibit users from accessing audit log entries, except those authorized users who have been granted explicit read-access, and b) prohibit users from modifying audit log entries. The system shall secure access to audit records and shall safeguard access to system audit tools and audit trails to prevent misuse or compromise, including deletion or modifications. **R61 Continuous Logging**: health information system audit logging shall be enabled at all times and there shall be no means for users to disable any audit logging. **R62 Preserving the History of personal health information**: The health information system shall not make deletions to records or audit log entries or changes to data subject records that prevent the reconstruction of records of a subject of care at a prior point in time.		
Software version control and documentation		
R63 health information system version control: all components of the health information system shall be identified and have an associated software version with a single unambiguous reference (unique ID, name, supplier, and version number). **R64 health information system documentation**: health information systems should have available documentation that addresses system requirements and capacities, installation and testing, management and operation, known security issues, user identification and authentication, privilege management and access control, secure communications, audit, software change management, time synchronization, and data backup and restoration. **R65 Changes to documentation**: documentation shall contain a history of all changes.	CSUP MLDP RDMP SAHD	8.6 Capacity management 8.7 Protection against malware 8.8 Management of technical vulnerabilities 8.9 Configuration management 8.17 Clock synchronization 8.18 Use of privileged utility programs 8.19 Installation of software on operational systems

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
R66 Documentation and software versions: all items of documentation shall clearly state at the beginning their version and the version of the software to which they apply. **R67 Software version**: health information systems shall have functionality that allows users to view the version of its software components. **R68 Topics included in documentation**: health information systems should have available documentation that addresses all of the following: a) system requirements, including services and network protocols that are necessary for proper operation, as well as the dependencies upon other EHR components; b) system product capacities (e.g. number of users, number of subjects of care, number of records, network load) and baseline representative configurations assumed for these capacities (e.g. number or type of processors, server/workstation configuration and network capacity); c) system installation, start-up, and connection, including communication security setup; d) steps needed to confirm that the system installation has been properly completed and that the system is operational; e) system management and operation; f) security mechanisms and practices, including creation, modification, and deactivation of user accounts; management of roles, reset of passwords, configuration of password constraints and other aspects of privilege management; communication security, and configuration and management of audit logs; g) known issues or conflicts with security services, including antivirus, malware eradication, intrusion detection, and firewalls, and the resolution of the conflict where applicable; h) software change management and hot-fix processes; i) system time (clock) synchronization where applicable; j) system error or performance messages to users and administrators, with required actions; k) data backup procedures, including data integrity checks when a backup copy is being produced or restored. **R69 Documentation and version control**: all health information system manuals shall clearly state, at the beginning of the document, the version(s) to which they apply. All updated health information system manuals should provide a summary for the reader of the changes since the last major revision. **R70 Changes to documentation**: documentation shall contain a history of all changes in a user readable form, so that users can check all changes made in the latest version available.		8.25 Secure development life cycle 8.26 Application security requirements 8.27 Secure system architecture and engineering principles 8.28 Secure coding 8.29 Security testing in development and acceptance 8.30 Outsourced development 8.31 Separation of development, test and production environments 8.32 Change management
Time synchronization and time/date formatting		

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
R71 Time format: health information systems shall adopt a uniform presentation of time for control and audit. **R72 Clock synchronization**: health information systems shall perform time synchronization using an accepted standard, and use this synchronized time in all records including times. **R73 Time format in exported records**: all time data for control and audit found in exported data (other than time stamp requests to, or responses from, a Time Stamping Authority) shall be represented in the ISO 8601:2019 format, indicating the difference between local time and UTC **R74 Secure time source**: health information systems shall use a consistent and secure time source.	AUDT CSUP SAHD	8.17 Clock synchronization
Privacy and security incident management		
R75 Incident management: health information systems or supporting audit systems shall trigger a configurable notification to the individual(s) or the security system in the organization accountable / responsible for managing privacy or security incidents each time a potential incidence of system misuse is detected. **R76 Incident notification:** health information systems should provide a facility so that users can notify an accountable person of security incidents or issues.	AUDT	5.5 Contact with authorities 5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events 5.26 Response to information security incidents 5.27 Learning from information security incidents 5.28 Collection of evidence 5.43 HLT – External incident reporting 6.8 Information security event reporting
Digital certificates and digital signatures		
R77 Providing digital signatures for users: health information systems that provide functions where users are required to apply the electronic equivalent of a handwritten signature should allow such users to apply a digital signature. **R78 Validating Digital Signatures**: whenever a health information system generates and receives data containing a digital signature, the system should confirm, at generation and upon receipt, that the signature is or was valid at the time it was applied. **R79 Preserving digital signatures**: health information systems that allow users to apply a digital signature or that receive digitally signed data, should store, backup or archive the digital signature whenever the signed data are stored, backed up or archived; and transmit the digital signature whenever the signed data are transmitted. **R80 Digital signing**: all health information systems providing functions where users are required to apply the electronic equivalent of a handwritten signature shall support a suitable digital signature standard compliant with information security policies and regulations. **R81 Validating, preserving and transmitting digital signatures**: the health information system shall:	AUDT PAUT TXCF TXIG	8.24 Use of cryptography

Table D.2 *(continued)*

Security and Privacy Requirements	IEC TS 81001-2-2	ISO 27799 Controls
a) confirm upon receipt that the signature is valid (i.e. that the associated signature certificate and all the associated chain certificates has not been revoked); b) store, backup or archive the digital signature and all related data (information about root certificates, certification chains, signatory certificates, and revocation information) whenever the signed data are stored, backed up or archived; c) transmit the digital signature together with the data or by reference whenever the signed data are transmitted; d) allow users to confirm, whenever they access signed data, that the signature is valid at the time of signing (i.e. that the associated signature certificate has not been revoked). **R82 Purpose of the signature and signatory role**: health information systems providing digital signature functionality should include the commitment-type-indication attribute and the role of the signatory (i.e. the user's role attribute).		

Table D.3 — Relationships between the ISO 27799 controls and the security and privacy requirements

ISO 27799 Control	Security and Privacy Requirements
5. Organizational controls	
5.1 Policies for information security	R1 Recording consent R2 Minimum data recorded R3 Directives follow the data R4 Emergency access: R5 Logging emergency access R6 Consent given by a legally authorized representative R7 Reporting changes to consent R8 Recording and storing only that data which has an identified purpose for its collection, use or disclosure R9 Limiting disclosure of data subject's information to healthcare providers with a relationship to the data subject R10 Restricting data exports R50 Record retention R56 Audit log retention R62 Preserving the history of personal health information
5.2 Information security roles & responsibilities 5.3 Segregation of duties 5.4 Management responsibilities 5.5 Contact with authorities 5.6 Contact with special interest groups	R25 Access controls R26 Authorization control R27 Role-based access control R28 Other forms of access control R29 Delegation of access to the personal health information of subjects of care R30 Reporting access privileges R31 Restrictions on access privileges R32 Revoking access privileges R75 Incident management R76 Incident notification
5.7 Threat intelligence	None

Table D.3 *(continued)*

ISO 27799 Control	Security and Privacy Requirements
5.8 Information security in project management	None
5.9 Inventory of information and other associated assets 5.10 Acceptable use of information and other associated assets 5.11 Return of assets	R33 Notifications to users R62 Preserving the history of personal health information
5.12 Classification of information 5.13 Labelling of information	R14 Subject of care identification R51 Labelling
5.14 Information transfer	R10 Restricting data exports R42 Encrypting data during transmission
5.15 Access control	R4 Emergency access R5 Logging emergency access R8 Recording and storing only that data which has an identified purpose for its collection, use or disclosure R9 Limiting disclosure of data subject's information to healthcare providers with a relationship to the data subject R10 Restricting data exports R27 Role-based access control R28 Other forms of access control R29 Delegation of access to the personal health information of subjects of care R30 Reporting access privileges R31 Restrictions on access privileges
5.16 Identity management	R15 User identification R16 User IDs
5.17 Authentication information	R17 User authentication R18 User authentication (prior to providing access to data or system services) R19 Authentication methods R20 User and system authentication R21 Protecting user profiles, passwords, and other authentication tokens R22 Passwords: use, quality, reset, and user changes R23 Failed Login Attempts R24 User feedback during authentication
5.18 Access rights	R25 Access controls R26 Authorization control R27 Role-based access control R28 Other forms of access control R29 Delegation of access to the personal health information of subjects of care R30 Reporting access privileges R31 Restrictions on access privileges R32 Revoking access privileges

Table D.3 *(continued)*

ISO 27799 Control	Security and Privacy Requirements
5.19 Information security in supplier relationships 5.20 Addressing information security within supplier agreements 5.21 Managing information security in the ICT supply chain 5.22 Monitoring, review and change management of supplier services 5.23 Information security for use of cloud services	None
5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events 5.26 Response to information security incidents 5.27 Learning from information security incidents 5.28 Collection of evidence	R75 Incident management R76 Incident notification
5.29 Information security during disruption 5.30 ICT readiness for business continuity	R48 Integrity of data during processing R57 Auditable events
5.31 Legal, statutory, regulatory & contractual requirements 5.32 Intellectual property rights	R68 Topics included in documentation
5.33 Protection of records 5.34 Privacy and protection of PII	R1 Recording consent R2 Minimum data recorded R3 Directives follow the data R4 Emergency access: R5 Logging emergency access R6 Consent given by a legally authorized representative R7 Reporting changes to consent R27 Role-based access control R29 Delegation of access to the personal health information of subjects of care R31 Restrictions on access privileges

Table D.3 *(continued)*

ISO 27799 Control	Security and Privacy Requirements
5.35 Independent review of information security 5.36 Compliance with policies, rules and standards for information security	R1 Recording consent R2 Minimum data recorded R3 Directives follow the data R4 Emergency access: R5 Logging emergency access R6 Consent given by a legally authorized representative R7 Reporting changes to consent R8 Recording and storing only that data which has an identified purpose for its collection, use or disclosure R9 Limiting disclosure of data subject's information to healthcare providers with a relationship to the data subject R10 Restricting data exports R50 Record retention R56 Audit log retention R62 Preserving the history of personal health information
5.37 Documented operating procedures	R68 Topics included in documentation
5.38 HLT – Information security requirements analysis and specification	R68 Topics included in documentation
5.39 HLT – Uniquely identifying subjects of care 5.40 HLT – Output data validation	R14 Subject of care identification
5.41 HLT – Publicly available health information	None
5.42 HLT – Emergency communication	None
5.43 HLT – External incident reporting	R75 Incident management R76 Incident notification
6. People controls	
6.1 Screening 6.2 Terms and conditions of employment 6.3 Information security awareness, education and training 6.4 Disciplinary process 6.5 Responsibilities after termination or change of employment 6.6 Confidentiality or non-disclosure agreements	None

Table D.3 *(continued)*

ISO 27799 Control	Security and Privacy Requirements
6.7 Remote working	R15 User authentication R16 User IDs R17 User authentication R18 User authentication (prior to providing access to data or system services) R19 Authentication methods R20 User and system authentication R21 Protecting user profiles, passwords, and other authentication tokens R22 Passwords: use, quality, reset, and user changes R23 Failed Login Attempts R24 User feedback during authentication R25 Access control R26 Authorization control R27 Role-based access control R29 Delegation of access to the personal health information of subjects of care R30 Reporting access privileges R31 Restrictions on access privileges R32 Revoking access privileges
6.8 Information security event reporting	R75 Incident management R76 Incident notification
6.9 HLT – Management training	None
7. Physical controls	
7.1 Physical security perimeters 7.2 Physical entry 7.3 Securing offices, rooms and facilities 7.4 Physical security monitoring 7.5 Protecting against physical and environmental threats 7.6 Working in secure areas 7.7 Clear desk and clear screen 7.8 Equipment siting and protection 7.9 Security of assets off-premises	R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositories
7.10 Storage media	R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositories
7.11 Supporting utilities 7.12 Cabling security 7.13 Equipment maintenance 7.14 Secure disposal or re-use of equipment	R45 Protecting data on portable media
8 Technological controls	

Table D.3 *(continued)*

ISO 27799 Control	Security and Privacy Requirements
8.1 User endpoint devices	R15 User identification R16 User IDs R17 User authentication R18 User authentication (prior to providing access to data or system services) R19 Authentication methods R20 User and system authentication R25 Access controls R34 Session security R35 User session timeout R36 Connection timeout R37 Session security R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositories
8.2 Privileged access rights 8.3 Information access restriction 8.4 Access to source code	R15 User identification R16 User IDs R17 User authentication R18 User authentication (prior to providing access to data or system services) R19 Authentication methods R20 User and system authentication R25 Access controls R26 Authorization control R27 Role-based access control R28 Other forms of access control R29 Delegation of access to the personal health information of subjects of care R30 Reporting access privileges R31 Restrictions on access privileges R32 Revoking access privileges
8.5 Secure authentication	R17 User authentication R18 User authentication (prior to providing access to data or system services) R19 Authentication methods R20 User and system authentication R21 Protecting user profiles, passwords, and other authentication tokens R22 Passwords: use, quality, reset, and user changes R23 Failed Login Attempts R24 User feedback during authentication R34 Session security
8.6 Capacity management 8.7 Protection against malware 8.8 Management of technical vulnerabilities 8.9 Configuration management	R68 Topics included in documentation R69 Documentation and version control R70 Changes to documentation
8.10 Information deletion	R50 Retention

Table D.3 *(continued)*

ISO 27799 Control	Security and Privacy Requirements
8.11 Data masking 8.12 Data leakage prevention	R21 Protecting user profiles, passwords, and other authentication tokens R32 Revoking access privileges R42 Encrypting data during transmission R43 Confirmation of data delivery R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositoriesR54 Protecting the audit log R58 Minimum content of information recorded
8.13 Information backup 8.14 Redundancy of information processing facilities	R38 Backup R39 Concurrent backup R40 Restoration R41 Reconstructing the content of an electronic health record at a prior point in time
8.15 Logging 8.16 Monitoring activities	R5 Logging emergency access R15 User identification R38 Backup R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositories R54 Protecting the audit log
8.17 Clock synchronization	R68 Topics included in documentation-clock synchronization-related requirement R71 Time format R72 Clock synchronization R73 Time format in exported records R74 Time source
8.18 Use of privileged utility programs 8.19 Installation of software on operational systems	R64 health information system documentation R68 Topics included in documentation-software installation-related requirements
8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks	R42 Encrypting data during transmission R43 Confirmation of data delivery
8.23 Web filtering	None
8.24 Use of cryptography	R21 Protecting user profiles, passwords, and other authentication tokens R42 Encrypting data during transmission R43 Confirmation of data delivery R77 Providing digital signatures for users R78 Validating Digital Signatures R79 Preserving digital signatures R80 Digital signing R81 Validating, preserving and transmitting digital signatures R82 Purpose of the signature and signatory role

Table D.3 *(continued)*

ISO 27799 Control	Security and Privacy Requirements
8.25 Secure development life cycle 8.26 Application security requirements 8.27 Secure system architecture and engineering principles 8.28 Secure coding 8.29 Security testing in development and acceptance 8.30 Outsourced development 8.31 Separation of development, test and production environments 8.32 Change management	R63 health information system version control R64 health information system documentation R65 Changes to documentation R66 Documentation and software versions R67 Software version R68 Topics included in documentation R69 Documentation and version control R70 Changes to documentation
8.33 Test information 8.34 Protection of information systems during audit testing	R44 Protecting operational data R45 Protecting data on portable media R46 Protecting data in data repositories R54 Protecting the audit log
8.35 HLT – Zero trust principles	None

Bibliography

[1] ISO 8601:2019, *(all parts), Date and time — Representations for information interchange*

[2] ISO/IEC 8859 (all parts), *Information technology — 8-bit single-byte coded graphic character sets*

[3] ISO/IEC 10646 (all parts), *Information technology — Universal coded character set (UCS)*

[4] ISO/IEEE 11073 (all parts), *Health informatics — Device interoperability*

[5] ISO 12052, *Health informatics — Digital imaging and communication in medicine (DICOM) including workflow and data management*

[6] ISO 13131, *Health informatics — Telehealth services — Quality planning guidelines*

[7] ISO 13940:2015, *Health informatics — System of concepts to support continuity of care*

[8] ISO/TS 14265, *Health informatics — Classification of purposes for processing personal health information*

[9] ISO 14441:2013, *Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment*

[10] ISO 17090-3, *Health informatics — Public key infrastructure — Part 3: Policy management of certification authority*

[11] ISO/TS 17975, *Health informatics — Principles and data requirements for consent in the collection, use or disclosure of personal health information*

[12] ISO 21089, *Health informatics — Trusted end-to-end information flows*

[13] ISO 21298, *Health informatics — Functional and structural roles*

[14] ISO/TR 21332, *Health informatics — Cloud computing considerations for the security and privacy of health information systems*

[15] ISO 22600 (all parts), *Health informatics — Privilege management and access control*

[16] ISO 22857, *Health informatics — Guidelines on data protection to facilitate trans-border flows of personal health data*

[17] ISO/TS 23535, *Health informatics — Requirements for customer-oriented health cloud service agreements*

[18] ISO 25237, *Health informatics — Pseudonymization*

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

[20] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[21] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[22] ISO 27789:2021, *Health informatics — Audit trails for electronic health records*

[23] ISO/HL7 27931, *Data Exchange Standards — Health Level Seven Version 2.5 — An application protocol for electronic data exchange in healthcare environments*

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

[25] IEC/TS 81001-2-2, *Health software and health IT systems safety, effectiveness and security — Guidance for the implementation, disclosure and communication of security needs, risks and controls*

[26] FHIR. *Fast Healthcare Interoperability Resources* —https://hl7.org/fhir/

[27] IHE. *Integrating the Healthcare Enterprise* — https://www.ihe.net

[28] World Health Organization (WHO). *WHO/HSS/EHT/DIM/11.03, Core Medical Equipment. Available at* https://iris.who.int/handle/10665/95788