norma española

UNE-EN ISO 27799:2016

Idioma: Inglés

TÍTULO

Informática sanitaria. Gestión de la seguridad de la información en sanidad utilizando la Norma ISO/IEC 27002 (ISO 27799:2016) (Ratificada por AENOR en octubre de 2016.)

TÍTULO INGLÉS

Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2016) (Endorsed by AENOR in October of 2016.)

TÍTULO FRANCÉS

Informatique de santé - Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002 (ISO 27799:2016) (Entérinée par l'AENOR en octobre 2016.)

OBSERVACIONES

En cumplimiento del punto 11.2.6.4 de las Reglas Internas de CEN/CENELEC Parte 2, se ha otorgado el rango de documento normativo español UNE al documento normativo europeo EN ISO 27799:2016 (Fecha de disponibilidad 2016-08-10)

Este documento está disponible en los idiomas oficiales de CEN/CENELEC/ETSI.

Este anuncio causará efecto a partir del primer día del mes siguiente al de su publicación en la revista AENOR.

La correspondiente versión oficial de este documento se encuentra disponible en AENOR (C/ Génova 6 28004 MADRID, www.aenor.es)

AENOR Asociación Española de Normalización y Certificación

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 27799

August 2016

ICS 35.240.80

Supersedes EN ISO 27799:2008

English Version

Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2016)

Informatique de santé - Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002 (ISO 27799:2016)

Medizinische Informatik - Informationsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 (ISO 27799:2016)

This European Standard was approved by CEN on 18 June 2016.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

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

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Ref. No. EN ISO 27799:2016 E

Contents

Page

European foreword

This document (EN ISO 27799:2016) has been prepared by Technical Committee ISO/TC 215 "Health informatics" in collaboration with Technical Committee CEN/TC 251 "Health informatics" the secretariat of which is held by NEN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2017, and conflicting national standards shall be withdrawn at the latest by February 2017.

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

This document supersedes EN ISO 27799:2008.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO 27799:2016 has been approved by CEN as EN ISO 27799:2016 without any modification.

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 documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 215, *Health informatics*.

This second edition cancels and replaces the first edition (ISO 27799:2008), which has been technically revised.

Introduction

This International Standard provides guidance to healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information. It is based upon and extends the general guidance provided by ISO/IEC 27002:2013 and addresses the special information security management needs of the health sector and its unique operating environments. While the protection and security of personal information is important to all individuals, corporations, institutions and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, auditability and availability of personal health information. This type of information is regarded by many as being among the most confidential of all types of personal information. Protecting this confidentiality is essential if the privacy of subjects of care is to be maintained. The integrity of health information is to be protected to ensure patient safety, and an important component of that protection is ensuring that the information's entire life cycle be fully auditable. The availability of health information is also critical to effective healthcare delivery. Health informatics systems is to meet unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks. Protecting the confidentiality, integrity and availability of health information therefore requires health sector specific expertise.

Regardless of size, location and model of service delivery, all healthcare organizations need to have stringent controls in place to protect the health information entrusted to them. Yet many health professionals work as solo health providers or in small clinics that lack the dedicated IT resources to manage information security. Healthcare organizations therefore need clear, concise, and health-care-specific guidance on the selection and implementation of such controls. This International Standard is to be adaptable to the wide range of sizes, locations, and models of service delivery found in healthcare. Finally, with increasing electronic exchange of personal health information between health professionals (including use of wireless and Internet services), there is a clear benefit in adopting a common reference for information security management in healthcare.

ISO/IEC 27002 is already being used extensively for health informatics IT security management through the agency of national or regional guidelines in Australia, Canada, France, the Netherlands, New Zealand, South Africa, the United Kingdom and elsewhere. ISO 27799 draws upon the experience gained in these national endeavours in dealing with the security of personal health information and is intended as a companion document to ISO/IEC 27002. It is not intended to supplant the ISO/IEC 27000-series of standards. Rather, it is a complement to these more generic standards.

ISO 27799 applies ISO/IEC 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health information. These considerations have, in some cases, led the authors to conclude that application of certain ISO/IEC 27002 control objectives is essential if personal health information is to be adequately protected. ISO 27799 therefore places constraints upon the application of certain security controls specified in ISO/IEC 27002.

All of the security control objectives described in ISO/IEC 27002 are relevant to health informatics, but some controls require additional explanation in regard to how they can best be used to protect the confidentiality, integrity and availability of health information. There are also additional health sector specific requirements. This International Standard provides additional guidance in a format that persons responsible for health information security can readily understand and adopt.

In the health domain, it is possible for an organization (a hospital, say) to be certified using ISO/IEC 27001 without requiring certification against or even acknowledgement of ISO 27799. It is to be hoped, however, that as healthcare organizations strive to improve the security of personal health information, conformance with ISO 27799 as a stricter standard for healthcare will also become widespread.

Objectives

Maintaining information confidentiality, availability, and integrity (including authenticity, accountability and auditability) are the overarching goals of information security. In healthcare, privacy of subjects of care depends upon maintaining the confidentiality of personal health information. To maintain

confidentiality, measures is also be taken to maintain the integrity of data, if for no other reason than that it is possible to corrupt the integrity of access control data, audit trails, and other system data in ways that allow breaches in confidentiality to take place or to go unnoticed. In addition, patient safety depends upon maintaining the integrity of personal health information, failure to do this can also result in illness, injury or even death. Likewise, a high level of availability is an especially important attribute of health systems, where treatment is often time-critical. Indeed, disasters that could lead to outages in other, non-health related, IT systems may be the very times when the information contained in health systems is most critically needed. Moreover, denial of service attacks against networked systems are increasingly common.

The controls discussed in this International Standard are those identified as appropriate in healthcare to protect confidentiality, integrity and availability of personal health information and to ensure that access to such information can be audited and accounted for. These controls help to prevent errors in medical practice that might ensue from failure to maintain the integrity of health information. In addition, they help to ensure that the continuity of medical services is maintained.

There are additional considerations that shape the goals of health information security. These includes the following:

a) honouring legislative obligations as expressed in applicable data protection laws and regulations protecting a subject of care is right to privacy;[1)]

b) maintaining established privacy and security best practices in health informatics;

c) maintaining individual and organizational accountability among health organizations and health professionals;

d) supporting the implementation of systematic risk management within health organizations;

e) meeting the security needs identified in common healthcare situations;

f) reducing operating costs by facilitating the increased use of technology in a safe, secure, and well managed manner that supports, but does not constrain current health activities;

g) maintaining public trust in health organizations and the information systems these organizations rely upon;

h) maintaining professional standards and ethics as established by health-related professional organizations (insofar as information security maintains the confidentiality and integrity of health information);

i) operating electronic health information systems in an environment appropriately secured against threats;

j) facilitating interoperability among health systems, since health information increasingly flows among organizations and across jurisdictional boundaries (especially as such interoperability enhances the proper handling of health information to ensure its continued confidentiality, integrity and availability).

Relation to information governance,[2)] corporate governance and clinical governance

While health organizations may differ in their positions on clinical governance and corporate governance, the importance of integrating and attending to information governance ought to be beyond debate as a vital support to both. As health organizations have become ever more critically dependent on information systems to support care delivery (e.g. by exploiting decision support technologies and trends towards “evidence based” rather than “experience based” healthcare), it has become evident that

1) In addition to legal obligations, a wealth of information is available on ethical obligations relating to health information, the code of ethics of the World Health Organization. These ethical obligations may also, in certain circumstances, impact health information security policy.

2) Note that in some countries, information governance is referred to as information assurance.

events in which losses of integrity, availability and confidentiality occur may have a significant clinical impact and that problems arising from such impacts will be seen to represent failures in the ethical and legal obligations inherent in a "duty of care".

All countries and jurisdictions will undoubtedly have case studies where such breaches have led to misdiagnoses, deaths, or protracted recoveries. Clinical governance frameworks need therefore to treat effective information security risk management as equal in importance to care treatment plans, infection management strategies and other "core" clinical management matters. This International Standard will assist those responsible for clinical governance in understanding the contribution made by effective information security strategies.

Health information to be protected

There are several types of information whose confidentiality, integrity and availability[3)] needs to be protected by

a) personal health information,

b) pseudonymized data derived from personal health information through some methodology for pseudonymous identification,

c) statistical and research data, including anonymized data derived from personal health information by removal of personally identifying data,

d) clinical/medical knowledge not related to any specific subjects of care, including clinical decision support data (e.g. data on adverse drug reactions),

e) data on health professionals, staff and volunteers,

f) information related to public health surveillance,

g) audit trail data, produced by health information systems, that contain personal health information or pseudonymous data derived from personal health information, or that contain data about the actions of users in regard to personal health information, and

h) system security data for health information systems, including access control data and other security related system configuration data, for health information systems.

The extent to which confidentiality, integrity and availability need to be protected depends upon the nature of the information, the uses to which it is put, and the risks to which it is exposed. For example, statistical data [item c) above] may not be confidential, but protecting its integrity may be very important. Likewise, audit trail data [item g) above] might not require high availability (frequent archiving with a retrieval time measured in hours rather than seconds might suffice in a given application) but its content might be highly confidential. Risk assessment can properly determine the level of effort needed to protect confidentiality, integrity and availability (see B.4.4). The results of regular risk assessment need to be fitted to the priorities and resources of the implementing organization.

Threats and vulnerabilities in health information security

Types of information security threats and vulnerabilities vary widely, as do their descriptions. While none are truly unique to healthcare, what is unique in healthcare is the array of factors to be considered when assessing threats and vulnerabilities.

By their nature, health organizations operate in an environment where visitors and the public at large can never be totally excluded. In large health organizations, the sheer volume of people moving through operational areas is significant. These factors increase the vulnerability of systems to physical threats. The likelihood that such threats will occur may increase when emotional or mentally ill subjects of care or relatives are present.

3) Level of availability depends upon the uses to which the data will be put.

The critical importance of correctly identifying subjects of care and correctly matching them to their health records leads health organizations to collect detailed identifying information. Regional or jurisdictional patient registries (i.e. registries of subjects of care) are sometimes the most comprehensive and up-to-date repositories of identifying information available in a jurisdiction. This identifying information is of great potential value to those who would use it to commit identity theft and so should be rigorously protected.

Many health organizations are chronically under-funded and their staff members are sometimes obliged to work under significant stress and with systems kept in service long after they ought to have been retired. These factors can increase the potential for certain types of threat and can exacerbate vulnerabilities. On the other hand, clinical care involves a range of professional, technical, administrative, ancillary and voluntary staff, many of whom see their work as a vocation. Their dedication and diversity of experience can often usefully reduce exposure to vulnerabilities. The high level of professional training received by many health professionals also sets healthcare apart from many other industrial sectors in reducing the incidence of insider threats.

The health environment, with its unique threats and vulnerabilities should therefore be considered with special care. Annex A contains an informative list of the types of threat that need to be considered by health organizations when they assess risks to the confidentiality, integrity and availability of health information and to the integrity and availability of related information systems.

Who should read this International Standard?

This International Standard is intended for those responsible for overseeing health information security and for healthcare organizations and other custodians of health information seeking guidance on this topic, together with their security advisors, consultants, auditors, vendors and third-party service providers.

This International Standards authors do not intend to write a primer on computer security, nor to restate what has already been written in ISO/IEC 27002 or in ISO/IEC 27001. There are many security requirements that are common to all computer-related systems, whether used in financial services, manufacturing, industrial control, or indeed in any other organized endeavour. A concerted effort has been made to focus on security requirements necessitated by the unique challenges of delivering electronic health information that supports the provision of care.

Benefits of using this International Standard

ISO/IEC 27002 is a broad and complex International Standard and its advice is not tailored specifically to healthcare. ISO 27799 allows for the implementation of ISO/IEC 27002 within health environments in a consistent fashion and with particular attention to the unique challenges that the health sector poses. By following it, healthcare organizations help to ensure that the confidentiality and integrity of data in their care is maintained, that critical health information systems remain available and that accountability for health information is upheld.

The adoption of this International Standard by healthcare organizations both within and among jurisdictions will assist interoperation and enable the safe adoption of new collaborative technologies in the delivery of healthcare. Secure and privacy-protective information sharing can significantly improve healthcare outcomes.

As a result of implementing this International Standard, healthcare organizations can expect to see the number and severity of their security incidents reduced, allowing resources to be redeployed to productive activities. IT security will thereby allow health resources to be deployed in a cost effective and productive manner. Indeed, research by the respected Information Security Forum and by market analysts has shown that good all-round security can have as much as a 2 % positive effect upon organizations' results.

Finally, a consistent approach to IT security, understandable by all involved in healthcare, will improve staff morale and increase the trust of the public in the systems that maintain personal health information.

How to use this International Standard

Readers not already familiar with ISO/IEC 27002 are urged to read the introductory clauses of that standard before continuing. The implementers of ISO 27799 is to read first thoroughly ISO/IEC 27002, as the text below will frequently refer the reader to the relevant clauses of that standard. The present International Standard cannot be fully understood without access to the full text of ISO/IEC 27002.

Readers seeking guidance on how to implement ISO/IEC 27002 in a health environment will find a practical action plan described in Annex B. No mandatory requirements are contained in this clause. Instead, general advice and guidance are given on how best to proceed with implementation of ISO/IEC 27002 in healthcare. The clause is organized around a cycle of activities (plan/do/check/act) that are described in ISO/IEC 27001 and that, when followed, will lead to a robust implementation of an information security management system.

Readers seeking specific advice on the security control security control categories and clauses described in ISO/IEC 27002 will find it in the clauses of this International Standard with the same clause number and title as is found in ISO/IEC 27002. This clause leads the reader through each of the eleven security control clauses of the ISO/IEC 27002. Minimum requirements are stated where appropriate and, in some cases, normative guidelines are set out on the proper application of certain ISO/IEC 27002 security controls to the protection of health information.

Once ISO/IEC 27002 has been put into place, the ongoing management is considered essential if the benefits of the International Standard are to be maintained. Clause 18 discusses compliance assessment and the requirements for ongoing information security management. Annex C contains a self-assessment matrix with regard to compliance.

This International Standard concludes with four informative appendices.

Annex A describes the general threats to health information. Annex B briefly describes a practical action plan for implementing complementary information security related International Standards. Annex C provides a checklist for compliance to ISO 27799. Clause 2 lists the standards that are cited in a normative way; the Bibliography lists other related standards in health information security.

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

1 Scope

This International Standard gives guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).

This International Standard defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that International Standard.[4)]

This International Standard provides implementation guidance for the controls described in ISO/IEC 27002 and supplements them where necessary, so that they can be effectively used for managing health information security. By implementing this International Standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information in their care.

This International Standard applies to health information in all its aspects, whatever form the information takes (words and numbers, sound recordings, drawings, video, and medical images), whatever means are used to store it (printing or writing on paper or storage electronically), and whatever means are used to transmit it (by hand, through fax, over computer networks, or by post), as the information is always be appropriately protected.

This International Standard and ISO/IEC 27002 taken together define what is required in terms of information security in healthcare, they do not define how these requirements are to be met. That is to say, to the fullest extent possible, this International Standard is technology-neutral. Neutrality with respect to implementing technologies is an important feature. Security technology is still undergoing rapid development and the pace of that change is now measured in months rather than years. By contrast, while subject to periodic review, International Standards are expected on the whole to remain valid for years. Just as importantly, technological neutrality leaves vendors and service providers free to suggest new or developing technologies that meet the necessary requirements that this International Standard describes.

As noted in the introduction, familiarity with ISO/IEC 27002 is indispensable to an understanding of this International Standard.

The following areas of information security are outside the scope of this International Standard:

a) methodologies and statistical tests for effective anonymization of personal health information;

b) methodologies for pseudonymization of personal health information (see Bibliography for a brief description of a Technical Specification that deals specifically with this topic);

c) network quality of service and methods for measuring availability of networks used for health informatics;

d) data quality (as distinct from data integrity).

4) This International Standard is consistent with the revised version of ISO/IEC 27002.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1
health informatics
scientific discipline that is concerned with the cognitive, information processing and communication tasks of healthcare practice, education and research, including the information science and technology to support these tasks

[SOURCE: ISO/TR 18307:2001, 3.73]

3.2
health information system
repository of information regarding the health of a subject of care in computer-processable form, stored and transmitted securely, and accessible by multiple authorised users

[SOURCE: ISO/TR 20514:2005]

3.3
healthcare
type of services provided by professionals or paraprofessionals with an impact on health status

[SOURCE: European Parliament, 1998, as cited by WHO]

3.4
healthcare organization
organization that provides healthcare services

[SOURCE: ISO/TR 18307:2001, 3.74]

3.5
health professional
person who is authorised by a recognised body to be qualified to perform certain health duties

[SOURCE: ISO 17090-1:2013]

3.6
identifiable person
one who can be identified, directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

[SOURCE: ISO 22857:2013, 3.7]

3.7
patient
subject of care (3.9) consisting of one person

3.8
personal health information
information about an identifiable person that relates to the physical or mental health of the individual

Note 1 to entry: To provision of health services to the individual and that may include:

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

b) information about payments or eligibility for health care 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 (e.g. a health professional) as 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, the identity of the individual who is the subject of the information cannot be ascertained from the information.

3.9
subject of care
one or more persons scheduled to receive, receiving, or having received a health service

[SOURCE: ISO 18308:2011, 3.47]

4 Structure of this International Standard

This International Standard provides guidance on the 14 security control clauses, 35 main security categories and 114 controls specified in ISO/IEC 27002. As with that International Standard, each clause defining security controls contains one or more main security categories. The order of the clauses and categories does not imply their importance. Depending on the circumstances, security controls from any or all clauses could be important, healthcare organizations applying this International Standard should identify controls applicable to their environment and business processes.

Each main security control category of ISO/IEC 27002 contains a control objective stating what is to be achieved and one or more controls that can be applied to achieve the control objective.

Readers of this International Standard are presumed to have access to the text of ISO/IEC 27002. Control descriptions in this International Standard are structured as follows:

Health-specific control

Defines the health-specific control statement, as stated in ISO/IEC 27002, to satisfy the control objective. If there is no health-specific control, this part is not shown.

Health-specific implementation guidance

Provides more detailed information to support the implementation of the control in a healthcare delivery environment to meet the control objective when protecting the confidentiality, integrity and availability of personal health information. If there is no health-specific guidance provided, the text states “No additional guidance for information security management in health.”

Other health-specific information

Provides further health-specific information that may need to be considered, for example references to other International Standards. If there is no other information to be provided, this part is not shown.

5 Information security policies

5.1 Management direction for information security

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

5.1.1 Policies for information security

Control

ISO/IEC 27002:2013, 5.1.1, applies.

Health-specific control

Organizations processing health information, including personal health information, shall have a written information security policy that is approved by management, published, and then communicated to all employees and relevant external parties.

Implementation guidance

ISO/IEC 27002:2013, 5.1.1, applies.

Health-specific implementation guidance

In addition to following the guidance, given by ISO/IEC 27002 on what an information security policy should contain, this policy should contain statements on:

a) the need for health information security;

b) the goals of health information security;

c) compliance scope, as described in Clause 18;

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 identification of processes and systems that are vital in health care (i.e. failure may lead to adverse patient effects).

Ideally, revision of the policy's contents will be driven by the findings of the organization's risk assessment, although the policy itself need only set direction, state principles and point to other International Standards, where the (more frequently changing) specifics are to be found.

In creating their information security policy document, health organizations will need to specifically consider the following factors, which are unique to the health sector:

a) the breadth of health information;

b) the rights and ethical responsibilities of staff, as agreed in law, and as accepted by members of professional bodies;

c) the rights of subjects of care, where applicable, to privacy and 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) the legitimate needs of clinicians and health organizations to be able to overcome normal security protocols when healthcare priorities, often linked to the incapacity of certain subjects of care to express their preferences, necessitate such overrides, also the procedures to be employed to achieve this;

f) the obligations of the respective health organizations, and of subjects of care, where healthcare is delivered on a “shared care” or “extended care” basis;

g) the protocols and procedures to be applied to the sharing of information for the purposes of research and clinical trials;

h) the arrangements for, and authority limits of, temporary staff, such as locums, students and “on-call” staff;

i) the arrangements and limitations placed upon access to personal health information by volunteers and support staff, such as clergy and charity personnel;

j) the implications of security measures on patient safety;

k) the implications of information security measures on the performance of health information systems.

Many health organizations have found it advantageous to make the policy document available to staff electronically via an information security area on the health organization’s Intranet.

Where the health organization obtains support from third-party organizations or collaborates with third parties, and especially where it receives services from other jurisdictions, the policy framework should include documented policy, controls and procedures that cover such interactions and that specify the responsibilities of all parties. In cases where personal data is crossing national or jurisdictional boundaries, the provisions of ISO 22857 should be applied.

Other information

ISO/IEC 27002:2013, 5.1.1, applies.

5.1.2 Review of the policies for information security

Control

ISO/IEC 27002:2013, 5.1.2, applies.

Health-specific control

The health organization’s information security policy should be subject to ongoing, staged review, such that the totality of the policy is addressed at least annually. The policy should be reviewed after the occurrence of a serious security incident.

Implementation guidance

ISO/IEC 27002:2013, 5.1.2, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, such review should address:

a) the changing nature of the health organization’s operations and the concomitant changes to risk profile and risk management needs;

b) the changes made to the IT infrastructure of the organization, and the concomitant changes these bring to the organization’s risk profile;

c) the changes identified in the external environment that similarly impact the organization’s 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 information privacy commissioners regarding the protection of personal health information;

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. privacy commissioners);

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.

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1 Information security roles and responsibilities

Control

ISO/IEC 27002:2013, 6.1.1, applies.

Health-specific control

Organizations processing personal health information shall:

a) clearly define and assign information security responsibilities;

b) have an information security management forum (ISMF) in place to ensure that there is clear direction and visible management support for security initiatives involving the security of health information, as described in B.3 and B.4.

At a minimum, at least one individual shall be responsible for health information security within the organization.

The health information security forum shall meet regularly, on a monthly or near-to-monthly basis. (Typically, it is most effective to meet at the mid-point between the meetings of the governance body into which the forum reports. This allows emergency matters to be taken to a suitable meeting within a short period.)

A formal scope statement shall be produced that defines the boundary of compliance activity in terms of people, processes, places, platforms and applications.

Implementation guidance

ISO/IEC 27002:2013, 6.1.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note the essential nature of management responsibility in organizations that are custodians of personal health information, as described in B.2. Accountability and coordination can only be maintained over the long term, if the organization has an explicit information security management infrastructure.

Whatever organizational structure is adopted, it is of critical importance that it be designed and structured to facilitate access by subjects of care (e.g. to make requests to obtain personal health information), to facilitate reporting within the organizational structure and to ensure timely delivery of information.

As noted in B.4.3, the organization's (virtual or actual) information security officer should, among other duties, report to the forum and provide it with secretariat services. The officer should be responsible for collating, publishing and commenting on the reports received by forum members.

Health organizations should publicise the scope statement widely within the organization, then review it and ensure it is adopted by the organization's information, clinical and corporate governance groups.

Other information

ISO/IEC 27002:2013, 6.1.1, applies.

6.1.2 Segregation of duties

Control

ISO/IEC 27002:2013, 6.1.2, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing personal health information should, where feasible, segregate duties and areas of responsibility in order to reduce opportunities for unauthorized modification or misuse of personal health information.

Implementation guidance

ISO/IEC 27002:2013, 6.1.2, applies.

Other information

ISO/IEC 27002:2013, 6.1.2, applies.

6.1.3 Contact with authorities

Control

ISO/IEC 27002:2013, 6.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 6.1.3, applies.

6.1.4 Contact with special interest groups

Control

ISO/IEC 27002:2013, 6.1.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.1.4, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 6.1.4, applies.

6.1.5 Information security in project management

Control

ISO/IEC 27002:2013, 6.1.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.1.5, applies.

Health-specific control

Healthcare project management should consider patient safety as a project risk in any project involving the processing of personal health information.

Health-specific implementation guidance

Patient safety is a critical component of any project risk assessment in a project involving the processing of personal health information. Risks to patient safety need to be carefully analysed and explicitly addressed.

Other health-specific information.

ISO/IEC 27002:2013, 6.1, applies.

6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1 Mobile device policy

Control

ISO/IEC 27002:2013, 6.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.2.1, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should:

a) specifically assess the risks involved when using mobile devices in healthcare;

b) prepare a policy on the precautions to be taken when using mobile computing devices, including guidance and restrictions on the use of personal devices within the organisation, together with controls to meet jurisdictional privacy requirements;

c) require their mobile users to adhere to this policy.

As noted in ISO/IEC 27002, mobile network wireless connections, while similar to those of wired networks, have some important differences from an information security point of view. Some wireless encryption protocols, such as wired equivalent privacy (WEP) are still in use despite known weaknesses

that render them largely ineffective. Moreover, information stored on mobile devices may not always be backed up (e.g. because of limited network bandwidth or because the devices are not connected at the times when backups are scheduled).

Other information

ISO/IEC 27002:2013, 6.2.1, applies.

6.2.2 Teleworking

Control

ISO/IEC 27002:2013, 6.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.2.2, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should:

a) prepare policy on the precautions to be taken when teleworking;

b) ensure that teleworking users of health information systems abide by this policy.

Some national jurisdictions (e.g. in Germany) have already placed restrictions on teleworking by health professionals.

It is important to consider that in healthcare, teleworking can cross jurisdictional borders and can even take place on board planes and ships situated beyond any national jurisdiction. Physicians already routinely e-mail medical images, etc. across boundaries to obtain specialist opinions. International teams involved in disaster relief may, in future, rely upon health information systems in jurisdictions other than their home jurisdiction. The legal and ethical considerations of doing this need to be taken into account in the design and deployment of health information systems (especially national systems) that may be used in this manner.

Other information

ISO/IEC 27002:2013, 6.2.2, applies.

7 Human resource security

7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 Screening

Control

ISO/IEC 27002:2013, 7.1.1, applies.

Health-specific controls

All organizations whose staff, contractors, or volunteers process (or are expected to process) personal health information should, as a minimum, verify the identity, current address and previous employment of such staff, contractors and volunteers at the time of job application.

Background verification checks on all candidates for employment should include a verification of applicable health professional qualifications, where such qualifications are professionally accredited (e.g. physicians, nurses, etc.)

When an individual is hired for a specific information security role, organizations should make sure the candidate:

a) has the necessary competence to perform the security role;

b) can be trusted to take the role, especially if the role is critical for the organization.

Implementation guidance

ISO/IEC 27002:2013, 7.1.1, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, all organizations whose staff, contractors, or volunteers process (or are expected to process) personal health information should, as a minimum, verify the identity, current address and previous employment of such staff, contractors and volunteers at the time of job applications.

7.1.2 Terms and conditions of employment

Control

ISO/IEC 27002:2013, 7.1.2, applies.

Health-specific control

In addition to the control given by ISO/IEC 27002, all organizations whose staff members are involved in processing personal health information should document such involvement in relevant job descriptions. Security roles and responsibilities, as laid down in the organization's information security policy, should also be documented in relevant job descriptions.

Special attention needs to be placed upon the roles and responsibilities of temporary or short-term staff such as locums, students, interns, etc.

Implementation guidance

ISO/IEC 27002:2013, 7.1.2, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should ensure that employees or contractors have a duty to report breaches of health information security or patient privacy.

It is important to know how and where to contact health professional staff, although, as some medical staff move on a regular basis, address details may have a limited value. Health organizations should therefore give consideration to the collection of a reasonable number of references and to undertaking other forms of check, by professional bodies and academic institutions.

Wherever possible, criminal background checks should be undertaken. Note that these might already be carried out as part of a health professional accreditation. See also 7.1.1.

Other information

ISO/IEC 27002:2013, 7.1.2, applies.

7.2 During employment

Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

7.2.1 Management responsibilities

Control

ISO/IEC 27002:2013, 7.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 7.2.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note the special emphasis that needs to 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. Such concerns often make up a large percentage of complaints from those with fears about the confidentiality of their personal health information. 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 needs to address these concerns.

Other information

ISO/IEC 27002:2013, 7.2.1, applies.

7.2.2 Information security awareness, education and training

Control

ISO/IEC 27002:2013, 7.2.2, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, all organizations processing personal health information shall ensure that information security education and training are provided on induction and, that regular updates in organizational security policies and procedures are provided to all employees and, where relevant, third-party contractors, researchers, students and volunteers who process personal health information.

Employees of the organization and, where relevant, third-party contractors should be made aware of disciplinary processes and consequences with respect to breaches of information security.

Implementation guidance

ISO/IEC 27002:2013, 7.2.2, applies.

Other information

ISO/IEC 27002:2013, 7.2.2, applies.

7.2.3 Disciplinary process

Control

ISO/IEC 27002:2013, 7.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 7.2.3, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, health organizations' disciplinary processes with respect to breaches of information security should follow procedures that are reflected in policy and thus known to the subject(s) of the disciplinary process. In addition to complying with applicable laws, such processes should comply with the agreements reached between health professionals and health professional bodies.

Other information

ISO/IEC 27002:2013, 7.2.3, applies.

7.3 Termination and change of employment

Objective: To protect the organization's interests as part of the process of changing or terminating employment.

7.3.1 Termination or change of employment responsibilities

Control

ISO/IEC 27002:2013, 7.3.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 7.3.1, applies.

Health-specific implementation guidance

It is important to note that in healthcare, many types of staff, doctors and nurses, commonly progress through training programmes and other "rotations" where their access rights can change fundamentally. To ensure the termination of previous rights that are no longer required for their role, such changes of employment should be initially processed in the same way as for individuals who are leaving the organization's employ.

Other information

ISO/IEC 27002:2013, 7.3.1, applies.

8 Asset management

8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

8.1.1 Inventory of assets

Control

ISO/IEC 27002:2013, 8.1.1, applies.

Health-specific control

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should:

a) account for health information assets (i.e. maintain an inventory of such assets);

b) have a designated custodian of these health information assets (see 8.1.2);

c) have rules for acceptable use of these assets that are identified, documented and implemented.

Implementation guidance

ISO/IEC 27002:2013, 7.3.1, applies.

Health-specific implementation guidance

Organizations processing health information should have rules for maintaining the currency of information assets (e.g. the currency of a drug database) and the integrity of these assets (e.g. the functional integrity of medical devices that record or report data).

Medical devices that record or report data may require special security considerations in relation to the environment in which they operate and to the electromagnetic emissions that occur during their operation. Such devices should be uniquely identified.

Other information

ISO/IEC 27002:2013, 7.3.1, applies.

8.1.2 Ownership of assets

Control

ISO/IEC 27002:2013, 8.1.2, applies.

Assets maintained in the inventory should be owned.

Implementation guidance

ISO/IEC 27002:2013, 8.1.2, applies.

Health-specific implementation guidance

It is important to note that while many information assets can be owned by in the conventional sense used in ISO/IEC 27002, the notion of ownership of personal health information is fraught with legal, ethical and policy-based issues. In many jurisdictions, individuals may have rights with respect to their own personal health information that limit or transcend any straightforward notion of "ownership" of this information by a healthcare organization or a health professional. Rather, healthcare organizations and health professionals are often viewed in relation to personal health information as custodians or trustees.

Other information

ISO/IEC 27002:2013, 8.1.2, applies.

8.1.3 Acceptable use of assets

Control

ISO/IEC 27002:2013, 8.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 8.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

8.1.4 Return of assets

Control

ISO/IEC 27002:2013, 8.1.4, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, all employees and contractors, upon termination of employment, shall return all personal health information in their possession that is in non-electronic form and ensure that all personal health information in their possession in electronic form is updated on relevant systems and then securely deleted from any devices on which it has resided.

Implementation guidance

ISO/IEC 27002:2013, 8.1.4, applies.

8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

8.2.1 Classification of information

Control

ISO/IEC 27002:2013, 8.2.1, applies.

Health-specific control

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should uniformly classify such data as confidential.

Implementation guidance

ISO/IEC 27002:2013, 8.2.1, applies.

Health-specific implementation guidance

Determining levels of protection for information assets in healthcare is complex and comparisons with government or military data classifications can be misleading. The following are important characteristics of information assets within healthcare.

a) The confidentiality of personal health information is often largely subjective, rather than objective. In other words, ultimately, only the data subject (i.e. the subject of care) can make a proper determination of the relative confidentiality of various fields or groupings of data. For example, a person escaping from an abusive relationship may consider his or her new address and phone number to be much more confidential than clinical data about setting his or her broken arm.

b) The confidentiality of personal health information is context-dependent. For example, the name and address of a subject of care in a list of admissions to a hospital's emergency department may not be considered especially confidential by that individual, yet the same name and address in a list of admissions to a clinic treating sexual impotence may be considered highly confidential by the individual.

c) The confidentiality of personal health information can shift over the lifetime of an individual's health record. For example, changing societal attitudes over the last 20 years have resulted in many subjects of care no longer considering their sexual orientation to be confidential. Conversely, attitudes toward drug and alcohol dependency have caused some subjects of care to consider addiction counselling data to be, if anything, even more confidential today than such data would have been considered 20 years ago.

Because one cannot predict the sensitivity of a given element of personal health information through all its uses and all the phases of its life cycle, all personal health information should be subject to suitably careful protection at all times. Note that while all personal health information should be uniformly

classified as confidential, practical considerations may necessitate identifying the records of subjects of care, who may be at elevated risk of access by those who do not have a need to know. Such individuals include employees of the organization itself (especially if their condition is one eliciting emotional behaviours), heads of government, celebrities, politicians, newsmakers and members of groups facing especially high risks (e.g. those with sexually transmitted diseases, or those whose personal health information contains information about genetic predisposition to serious illness). The records of such individuals may need to be specially tagged so that access can be closely monitored. However, great care should be exercised in implementing such schemes as this tagging can exacerbate the very problem it is designed to avoid, i.e. it can draw attention to the particular data items tagged. It is also important to emphasize that while certain subjects of care may be at elevated risk, their personal health information is not innately more confidential than that of other subjects of care. All personal health information is confidential and should be treated accordingly. See also, the discussion in 7.2.1.

Identifying and (where appropriate) protectively labelling information assets as confidential can be an important tool in staff training and in policy compliance. This works best when the classification acts as an indicator of required information handling practices. The classification may also be an important component of data protection agreements among jurisdictions and with third-party organizations and their staff. The identification and labelling of information assets is also an essential component of ISO/IEC 27002.

In addition to the traditional classification of data on the basis of its sensitivity to disclosure, the criticality of information also needs to be classified, the extent to which the availability and integrity of the information are essential for the ongoing provision of healthcare. Time factors involved in clinical processes often play a crucial role in determining the availability requirements for personal health information. Classification in respect of availability, integrity and criticality also needs to be applied to processes, IT devices, software, locations and personnel. Criticality should be identified through a risk assessment.

Other information

ISO/IEC 27002:2013, 8.2.1, applies.

8.2.2 Labelling of information

Control

ISO/IEC 27002:2013, 8.2.2, applies.

Health-specific control

All health information systems processing personal health information should inform users of the confidentiality of personal health information accessible from the system (e.g. at start-up or log-in) and should label hardcopy output as confidential when it contains personal health information.

Implementation guidance

ISO/IEC 27002:2013, 8.2.2, applies.

Health-specific implementation guidance

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 contains personal health information.

Other information

ISO/IEC 27002:2013, 8.2.2, applies.

8.2.3 Handling of assets

Control

ISO/IEC 27002:2013, 8.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 8.2.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

8.3 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

8.3.1 Management of removable media

Control

ISO/IEC 27002:2013, 8.3.1, applies.

Health-specific control

In addition to the guidance given by ISO/IEC 27002, media containing personal health information shall be either physically protected or else have their data encrypted. The status and location of media containing unencrypted personal health information shall be monitored.

Implementation guidance

ISO/IEC 27002:2013, 8.3.1, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should ensure that all personal health information stored on removable media is

a) encrypted while its media are in transit, or

b) protected from theft while its media are in transit.

8.3.2 Disposal of media

Control

ISO/IEC 27002:2013, 8.3.2, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, all personal health information shall be securely erased or else the media destroyed when no longer required for use.

Implementation guidance

ISO/IEC 27002:2013, 8.3.2, applies.

Health-specific implementation guidance

Improper disposal of media continues to be a source of serious breaches of patient confidentiality. It is especially important to note that this control should be applied prior to the repair or disposal of any associated equipment. This requirement also applies to medical devices that record or report data.

Other information

ISO/IEC 27002:2013, 8.3.21, applies.

8.3.3 Physical media transfer

Control

ISO/IEC 27002:2013, 8.3.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 8.3.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 8.3.3, applies.

9 Access control

9.1 Business requirements of access control

Objective: To limit access to information and information processing facilities.

9.1.1 Access control policy

Control

ISO/IEC 27002:2013, 9.1.1, applies.

Health-specific control

Organizations processing personal health information shall control access to such information. In general, users of health information systems should only access personal health information:

a) when a healthcare relationship exists between the user and 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.

Organizations processing personal health information shall have an access control policy governing access to these data.

The organization's policy on access control should be established on the basis of predefined roles with associated authorities which are consistent with, but limited to, the needs of that role.

The access control policy, as a component of the information security policy framework described in 5.1.1, shall reflect professional, ethical, legal and subject-of-care-related requirements and should take account of the tasks performed by health professionals and the task's workflow.

The organization should identify and document all parties with whom patient data is exchanged and contractual agreements should be made with these parties regulating access and privileges, prior to exchange of patient data.

Implementation guidance

ISO/IEC 27002:2013, 9.1.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note that, in order that healthcare delivery not be delayed or baulked, there are stronger requirements than usual for a clear policy and process, with associated authorization, to override the "normal" access control rules in emergency situations.

Health organizations are encouraged to consider the implementation of a federated identity and access management solution in recognition of the potential additional support, and reduced administration costs, that this will provide to the access control policy. Additionally, this will support higher-level security access processes, such as smart-card-based access and "single-sign-on" capability.

Other information

ISO/IEC 27002:2013, 9.1.1, applies.

Other health-specific information

Additional guidance on access control in healthcare-related applications can be found in ISO 22600.

9.1.2 Access to networks and network services

Control

ISO/IEC 27002:2013, 9.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.1.2, applies.

Other information

ISO/IEC 27002:2013, 9.1.2, applies.

9.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

9.2.1 User registration and de-registration

Control

ISO/IEC 27002:2013, 9.2.1, applies.

Health-specific control

Access to health information systems that process personal health information shall be subject to a formal user registration process. User registration procedures shall ensure that the level of authentication required of claimed user identity is consistent with the level(s) of access that will become available to the user.

User registration details shall be periodically reviewed to ensure that they are complete, accurate and that access is still required.

Implementation guidance

ISO/IEC 27002:2013, 9.2.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to understand that the task of identifying and registering users of health information systems includes all of the following:

a) the accurate capture of a user's identity (e.g. Joan Smith, born March 26th 1982, currently resident at a specific address);

b) the accurate capture, after verification, of a user's enduring professional credentials (e.g. Dr. Joan Smith, cardiologist) and/or job title (e.g. Susan Jones, Medical Receptionist);

c) the assignment of an unambiguous user identifier.

Note that subjects of care are not typically system users, although those who are able to access all or part of their personal data online (e.g. through an online portal) would indeed be system users (though ones who are granted limited access). Note also that there are health applications where a user may seek general health advice and information. While this request for information may be recorded, the accessing user remains anonymous. Many Web sites offering information on pregnancy, AIDS, or other public health topics operate in this fashion. Users of such general information sites do not typically require registration and are therefore excluded from consideration in the discussion that follows. See also 7.2.1.

Other information

ISO/IEC 27002:2013, 9.2.1, applies.

9.2.2 User access provisioning

Control

ISO/IEC 27002:2013, 9.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.2.2, applies.

Health-specific implementation guidance

User access provisioning procedures should clearly determine whether users will or will not have access to personal health information.

Other information

ISO/IEC 27002:2013, 9.2.2, applies.

9.2.3 Management of privileged access rights

Control

ISO/IEC 27002:2013, 9.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.2.3, applies.

Health-specific implementation guidance

In the discussion that follows, several access control strategies are specified that can help significantly to ensure the confidentiality and integrity of personal health information. These are:

a) role-based access control, which relies upon the professional credentials and job titles of users established during registration to restrict users' access privileges to just those required to fulfil one or more well-defined roles;

b) workgroup-based access control, which relies upon the assignment of users to workgroups (such as clinical teams) to determine which records they can access;

c) discretionary access control, which enables users of health information systems who have a legitimate relationship to a subject of care's personal health information (e.g. a family physician) to grant access to other users who have no previously established relationship to that subject of care's personal health information (e.g. a specialist).

In addition to following the guidance given by ISO/IEC 27002, health information systems containing personal health information should support role-based access control capable of mapping each user to one or more roles and each role to one or more system functions.

A user of a health information system containing personal health information shall access its services in a single role (i.e. users who have been registered with more than one role shall designate a single role during each health information system access session).

Health information systems should associate users (including health professionals, supporting staff and others) with the records of subjects of care and allow future access based on this association.

Additional guidance on privilege management in health can be found in ISO 22600-1 and in ISO 22600-2.

<u>Other information</u>

ISO/IEC 27002:2013, 9.2.3, applies.

9.2.4 Management of secret authentication information of users

<u>Control</u>

ISO/IEC 27002:2013, 9.2.4, applies.

<u>Implementation guidance</u>

ISO/IEC 27002:2013, 9.2.4, applies.

<u>Health-specific implementation guidance</u>

No additional guidance for information security management in health, although it should be noted that time pressures found in health delivery situations can make effective use of passwords difficult to employ. Many health organizations have considered the adoption of alternative authentication technologies to address this problem.

<u>Other information</u>

ISO/IEC 27002:2013, 9.2.4, applies.

9.2.5 Review of user access rights

<u>Control</u>

ISO/IEC 27002:2013, 9.2.5, applies.

<u>Implementation guidance</u>

ISO/IEC 27002:2013, 9.2.5, applies.

<u>Health-specific implementation guidance</u>

In addition to the guidance given by ISO/IEC 27002, special consideration needs to be given to users who will reasonably be expected to provide emergency care, as they may need access to personal health information in emergency situations, where a subject of care may be unable to communicate consent.

<u>Other information</u>

ISO/IEC 27002:2013, 9.2.5, applies.

9.2.6 Removal or adjustment of access rights

Control

ISO/IEC 27002:2013, 9.2.6, applies.

Health-specific control

All organizations that process personal health information shall, as soon as possible, terminate the user access privileges with respect to such information for any departing permanent or temporary employee, third-party contractor or volunteer upon termination of employment, contracting, or volunteer activities.

Implementation guidance

ISO/IEC 27002:2013, 9.2.6, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note the many examples in healthcare of students, interns and locums who have retained their access privileges after cessation of their internship, locum, etc. Especially in large hospitals, large numbers of temporary 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. At the same time, in healthcare, many transactions take place well after the time of care (e.g. the sign-off of medical transcriptions). 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.

Health organizations should seriously consider immediate termination of access rights following the supply of a resignation notice, notice of dismissal, etc. wherever an increased risk is perceived from the continuation of such access.

Other information

ISO/IEC 27002:2013, 9.2.6, applies.

9.3 User responsibilities

Objective: To make users accountable for safeguarding their authentication information.

9.3.1 Use of secret authentication information

Control

ISO/IEC 27002:2013, 9.3.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.3.1, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing health information should, when determining user responsibilities, respect the rights and ethical responsibilities of health professionals, as agreed in law and as accepted by members of health professional bodies.

Other information

ISO/IEC 27002:2013, 9.3.1, applies.

9.4 System and application access control

Objective: To prevent unauthorized access to systems and applications.

9.4.1 Information access restriction

Control

ISO/IEC 27002:2013, 9.4.1, applies.

Health-specific control

Health information systems processing personal health information shall authenticate users and should do so by means of authentication involving at least two factors.

Access to information and application system functions related to the processing personal health information should be isolated from (and separate to) access to information processing infrastructure that is unrelated to the processing of personal health information.

Implementation guidance

ISO/IEC 27002:2013, 9.4.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, special consideration should be given to the technical measures by which a subject of care is securely authenticated when accessing all or part of his/her own information (in those health information systems that permit such access). Similar emphasis should also be given to the ease of use of such measures, especially for handicapped subjects of care, and to provisions for access by substitute decision makers.

9.4.2 Secure log-on procedures

Control

ISO/IEC 27002:2013, 9.4.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.4.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 9.4.2, applies.

9.4.3 Password management system

Control

ISO/IEC 27002:2013, 9.4.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.4.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 9.4.3, applies.

9.4.4 Use of privileged utility programs

Control

ISO/IEC 27002:2013, 9.4.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.4.4, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 9.4.4, applies.

9.4.5 Access control to program source code

Control

ISO/IEC 27002:2013, 9.4.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.4.5, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

10 Cryptography

10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

10.1.1 Policy on the use of cryptographic controls

Control

ISO/IEC 27002:2013, 10.1.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 10.1.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, guidance on policy for the issuance and use of digital certificates in healthcare and on the management of keys can be found in ISO 17090-3.

Other information

ISO/IEC 27002:2013, 10.1.1, applies.

10.1.2 Key management

Control

ISO/IEC 27002:2013, 10.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 10.1.2, applies.

Health-specific implementation guidance

Guidance on key management can be found in ISO 17090-3.

Other information

ISO/IEC 27002:2013, 10.1.1, applies.

11 Physical and environmental security

11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

11.1.1 Physical security perimeter

Control

ISO/IEC 27002:2013, 11.1.1, applies.

Health-specific control

Organizations processing personal health information should use security perimeters to protect areas that contain information processing facilities supporting such health applications. These secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Implementation guidance

ISO/IEC 27002:2013, 11.1.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to acknowledge that in many healthcare settings, the instantiation of security perimeters is especially challenging. Many operational areas are permeated by subjects of care. Indeed, there is perhaps no other industrial sector where the public has more extensive access to operational areas than in healthcare. At the same time, a safe environment needs to be maintained that preserves the physical safety and security of subjects of care, as well as of the data and systems that may be accessible within that environment. For example, a patient may be left unattended in an examining room (e.g. to allow the patient 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 patients from a security perimeter. This is in contrasts with a bank where customers might never be left unattended in areas with functioning workstations. Moreover, unlike clients of other industrial sectors, clients in healthcare are often unable to physically provide for their own personal safety and security.

Physical security measures for information should be coordinated with physical security and safety measures for subjects of care. Healthcare organizations have a duty to protect both.

Other information

ISO/IEC 27002:2013, 11.1.1, applies.

11.1.2 Physical entry controls

Control

ISO/IEC 27002:2013, 11.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 11.1.2, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations that process personal health information should take sensible steps to ensure that the public are only as close to IT equipment (servers, storage devices, terminals and displays) as physical constraints and clinical processes demand.

11.1.3 Securing offices, rooms and facilities

Control

ISO/IEC 27002:2013, 11.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 11.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

11.1.4 Protecting against external and environmental threats

Control

ISO/IEC 27002:2013, 11.1.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 11.1.4, applies.

Health-specific implementation guidance

See the health-specific implementation guidance in 11.1.2.

11.1.5 Working in secure areas

Control

ISO/IEC 27002:2013, 11.1.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 11.1.5, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

11.1.6 Delivery and loading areas

Control

ISO/IEC 27002:2013, 11.1.6, applies.

Implementation guidance

ISO/IEC 27002:2013, 11.1.6, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note that the provision of healthcare includes distinct circumstances where the public (subjects of care and their support companions) are physically admitted into areas with vast amounts of sensitive information (e.g. laboratory testing where workflow may dictate gathering information from subjects of care in the same area where data from previous subjects is currently being processed, emergency room treatment areas where companions or relatives could potentially be exposed to significant amounts of sensitive verbal and visual information on other subjects of care; bedside computing/nursing workstations located near patient rooms). Those physical areas in healthcare that gather health information through interview and that contain systems where data are viewed on screen should therefore be subject to additional scrutiny.

To ensure that the privacy of subjects of care is maintained, healthcare often requires that notices be posted in lifts, on doors behind which interviews may be conducted and in other areas. Such notices serve as a reminder to curtail discussion of patient cases in public areas.

11.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

11.2.1 Equipment siting and protection

Control

ISO/IEC 27002:2013, 11.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 11.2.1, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should situate any workstations allowing access to personal health information in a way that prevents unintended viewing or access by subjects of care and the public.

Medical devices that record or report data may also require special security considerations in relation to the environment in which they operate and to the electromagnetic emissions that occur during their operation. Healthcare organizations, especially hospitals, should ensure that the siting and protection guidelines for IT equipment minimize exposure to such emissions.

11.2.2 Supporting utilities

Control

ISO/IEC 27002:2013, 11.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 11.2.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 11.2.2, applies.

11.2.3 Cabling security

Control

ISO/IEC 27002:2013, 11.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 11.2.3, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, health organizations should give serious consideration to the shielding of network and other cabling in areas with high emissions from medical devices.

11.2.4 Equipment maintenance

Control

ISO/IEC 27002:2013, 11.2.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 11.2.4, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, health organizations should give serious consideration to the shielding of equipment in areas with high emissions from medical devices.

11.2.5 Removal of assets

Control

ISO/IEC 27002:2013, 11.2.5, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations providing or using equipment, data or software to support a healthcare application containing personal health information shall not allow such equipment, data, or software to be removed from the site or relocated within it without authorization by the organization.

Implementation guidance

ISO/IEC 27002:2013, 11.2.5, applies.

Other information

ISO/IEC 27002:2013, 11.2.5, applies.

11.2.6 Security of equipment and assets off-premises

Control

ISO/IEC 27002:2013, 11.2.6, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing personal health information shall ensure that any use, outside its premises, of medical devices that record or report data has been authorized. This should include equipment used by remote workers, even where such usage is perpetual (i.e. where it forms a core feature of the employee's role, such as for ambulance personnel, therapists, etc.)

Implementation guidance

ISO/IEC 27002:2013, 11.2.6, applies.

Other information

ISO/IEC 27002:2013, 11.2.6, applies.

11.2.7 Secure disposal or reuse of equipment

Control

ISO/IEC 27002:2013, 11.2.7, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing health information applications shall securely erase or else destroy all media containing health information application software or personal health information when the media are no longer required for use.

Implementation guidance

ISO/IEC 27002:2013, 11.2.7, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 11.2.7, applies.

11.2.8 Unattended user equipment

Control

ISO/IEC 27002:2013, 11.2.8, applies.

Implementation guidance

ISO/IEC 27002:2013, 11.2.8, applies.

Health-specific implementation guidance

No additional guidance for information security management in health. See also 9.3.

11.2.9 Clear desk and clear screen policy

Control

ISO/IEC 27002:2013, 11.2.9, applies.

Implementation guidance

ISO/IEC 27002:2013, 11.2.9, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing health information should, when determining user responsibilities, respect the rights and ethical responsibilities of health professionals, as agreed in law and as accepted by members of health professional bodies. See also 9.3.

Other information

ISO/IEC 27002:2013, 11.2.9, applies.

12 Operations security

12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities.

12.1.1 Documented operating procedures

Control

ISO/IEC 27002:2013, 12.1.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.1.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

12.1.2 Change management

Control

ISO/IEC 27002:2013, 12.1.2, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing personal health information shall, by means of a formal and structured change control process, control changes to information processing facilities and systems that process personal health information to ensure the appropriate control of host applications and systems and continuity of patient care.

Implementation guidance

ISO/IEC 27002:2013, 12.1.2, applies.

Health-specific implementation guidance

It is important to note that inappropriate, inadequately tested or incorrect changes to the processing of personal health information can have disastrous consequences for patient care and safety. The change process should explicitly record and assess the risks of the change.

Other information

ISO/IEC 27002:2013, 12.1.2, applies.

Other health-specific information

ISO/TS 14441 contains detailed guidance on conformance testing of EHR systems, including use of test data.

12.1.3 Capacity management

Control

ISO/IEC 27002:2013, 12.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 12.1.3, applies.

12.1.4 Separation of development, testing and operational environments

Control

ISO/IEC 27002:2013, 12.1.4, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing personal health information shall separate (physically or virtually) development and testing environments for health information systems processing such information from operational environments hosting those health information systems. Rules for the migration of software from development to operational status shall be defined and documented by the organization hosting the affected application(s).

Implementation guidance

ISO/IEC 27002:2013, 12.1.4, applies.

Other information

ISO/IEC 27002:2013, 12.1.4, applies.

12.2 Protection from malware

Objective: To ensure that information and information processing facilities are protected against malware.

12.2.1 Controls against malware

Control

ISO/IEC 27002:2013, 12.2.1, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing personal health information shall implement appropriate prevention, detection and response controls to protect against malicious software and shall implement appropriate user awareness training.

Implementation guidance

ISO/IEC 27002:2013, 12.2.1, applies.

Other information

ISO/IEC 27002:2013, 12.2.1, applies.

12.3 Backup

Objective: To protect against loss of data.

12.3.1 Information backup

Control

ISO/IEC 27002:2013, 12.3.1, applies.

Health-specific control

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information shall back up all personal health information and store it in a physically secure environment to ensure its future availability.

To protect its confidentiality, personal health information should be backed up in an encrypted format.

Implementation guidance

ISO/IEC 27002:2013, 12.3.1, applies.

12.4 Logging and monitoring

Objective: To record events and generate evidence.

12.4.1 Event logging

Control

ISO/IEC 27002:2013, 12.4.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.4.1, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, health information systems processing personal health information should create a secure audit record each time a user accesses, creates, updates or archives personal health information via the system. The audit log should uniquely identify the user, uniquely identify the data subject (i.e. the subject of care), identify the function performed by the user (record creation, access, update, etc.), and note the time and date at which the function was performed.

When personal health information is updated, a record of the former content of the data and the associated audit record (i.e. who entered the data on what date) should be retained.

Messaging systems used to transmit messages containing personal health information should keep a log of message transmissions (such a log should contain the time, date, origin and destination of the message, but not its content).

The organization should carefully assess and determine the retention period for these audit logs, with particular reference to clinical professional standards and legal obligations, in order to enable investigations to be carried out when necessary and to provide evidence of misuse where necessary.

The health information system’s audit logging facility should be operational at all times while the health information system being audited is available for use.

Health information systems containing personal health information should be provided with facilities for analysing logs and audit trails that:

a) allow the identification of all system users who have accessed or modified a given subject of care's record(s) over a given period of time;

b) allow the identification of all subjects of care whose records have been accessed or modified by a given system user over a given period of time.

Other information

ISO/IEC 27002:2013, 12.4.1, applies.

Other health-specific information

Of all security requirements protecting personal health information, among the most important are those relating to audit and logging. These ensure accountability for subjects of care entrusting their information to electronic health record systems and also provide a strong incentive to users of such systems to conform to the policies on the acceptable use of these systems. Effective audit and logging can help to uncover misuse of health information systems or of personal health information. These processes can also help organizations and subjects of care to obtain redress against users abusing their access privileges.

Requirements for event logging are addressed in detail in ISO 27789.

12.4.2 Protection of log information

Control

ISO/IEC 27002:2013, 12.4.2, applies.

Health-specific control

Audit records shall be secure and tamper-proof. Access to system audit tools and audit trails shall be safeguarded to prevent misuse or compromise.

Implementation guidance

ISO/IEC 27002:2013, 12.4.2, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note that the evidentiary integrity of audit records can play an essential role in coroners' inquests, investigations into medical malpractice, and other judicial or quasi-judicial proceedings. In such proceedings, the actions of health professionals and the timing of events are sometimes determined through an examination of changes and updates to an individual's personal health information.

In relation to the maintenance of confidentiality and integrity of health records and the integrity and availability of health information systems, the following criteria are stated in IETF RFC 3881:

> Audit data shall be secured at least to the same extent as the underlying data and activities being audited. This includes access controls as well as data integrity and recovery functions. This document acknowledges the need for, but does not specify, the policies and technical methods to accomplish this.
>
> It is conceivable that audit data might have unintended uses, e.g. tracking the frequency and nature of system use for productivity measures. ASTM standard E2147-01 states, in 5.3.10, "Prohibit use for other reasons than to enforce security and to detect security breaches in record health information systems, for example, the audits are not to be used to explore activity profiles or movement profiles of employees."

Management of audit records should follow the International Standard on records management ISO 15489. Security requirements for archiving of audit records are similar to those for archiving of electronic health records specified in ISO/TS 21547.

Special attention should be given to the security of distributed audit trails. Whereas electronic health records may be distributed over multiple information systems and spanning distinct security policy domains this also pertains to audit trails. Security should be maintained over the logical audit trails.

The audit system shall provide sufficient measures to ensure that entries are made in the audit trail whenever the health information system is operational.

The audit system shall document all instances when the audit trail has been out of service, turned off or not functional by a system failure.

The audit system shall show or report which audits are on/off at any given time.

An organization responsible for the maintaining an audit log shall define the retention policy governing the audit records.

Retention of the audit records should follow legal requirements and relevant policies.

Retention of the audit records should support the life of the health records, data and documents.

The audit system shall provide sufficient security measures to protect audit logs from tampering. In particular,

a) it shall secure access to audit records,

b) it shall safeguard access to system audit tools to prevent misuse or compromise,

c) it shall keep track of all actions to the audit trail by a secure log specifying time, action and actor,

d) it shall document all occasions when the audit trail has been out of service, turned off or by a system failure, and

e) it shall report of which audits are on/off at any given time.

Access to audit data needs to 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.

Auditing facilities should provide analysis of the audit trail by any of the data fields within the log, by date/time period where appropriate, either individually or in combination (e.g. all access by user X, all "delete" events by users of role "Y", all events involving subject of care "Z" in the past month, etc.).

In some cases, it may be necessary for an audit user to access information sources in addition to the audit trail, for example, to spot patterns (e.g. all searches on children carried out by a user who is not a paediatrician or affiliated with paediatrics).

<u>Other information</u>

ISO/IEC 27002:2013, 12.4.2, applies.

<u>Other health-specific information</u>

Guidance on long-term archiving while assuring data integrity guidance is also given in the documents IETF RFC 4810 Long-Term Archive Service Requirements and IETF RFC 4998 Evidence Record Syntax (ERS).

12.4.3 Administrator and operator logs

<u>Control</u>

ISO/IEC 27002:2013, 12.4.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.4.3, applies.

Other information

ISO/IEC 27002:2013, 12.4.3, applies.

12.4.4 Clock synchronisation

Control

ISO/IEC 27002:2013, 12.4.4, applies.

Health-specific control

Health information systems supporting time-critical-shared care activities shall provide time synchronization services to support tracing and reconstitution of activity timelines where required.

Implementation guidance

ISO/IEC 27002:2013, 12.4.4, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note that the timing of events as electronically recorded in personal health information and in audit records can play an essential role in processes, such as coroners' inquests, investigations into medical malpractice and other judicial or quasi-judicial proceedings where it is essential to accurately determine a clinical sequence of events.

Other information

ISO/IEC 27002:2013, 12.4.4, applies.

12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

Control

ISO/IEC 27002:2013, 12.5.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.5.1, applies.

12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

12.6.1 Management of technical vulnerabilities

Control

ISO/IEC 27002:2013, 12.6.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.6.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 12.6.1, applies.

12.6.2 Restrictions on software installation

Control

ISO/IEC 27002:2013, 12.6.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.6.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 12.6.2, applies.

12.7 Information systems audit considerations

Objective: To minimise the impact of audit activities on operational systems.

12.7.1 Information systems audit controls

Control

ISO/IEC 27002:2013, 12.7.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 12.7.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

13 Communications security

13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

13.1.1 Network controls

Control

ISO/IEC 27002:2013, 13.1.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.1.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 13.1.1, applies.

13.1.2 Security of network services

Control

ISO/IEC 27002:2013, 13.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.1.2, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should carefully consider what impact the loss of network service availability will have upon clinical practice. See also Clause 17.

Other information

ISO/IEC 27002:2013, 13.1.2, applies.

13.1.3 Segregation in networks

Control

ISO/IEC 27002:2013, 13.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 13.1.3, applies.

13.2 Information transfer

Objective: To maintain the security of information transferred within an organization and with any external entity.

13.2.1 Information transfer policies and procedures

Control

ISO/IEC 27002:2013, 13.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.2.1, applies.

Health-specific implementation guidance

Organizations shall ensure that the security of such exchanges of information is the subject of policy development and compliance audit (see Clause 18).

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.

Special attention should be given to the usability of cryptographic tools. If such tools are too complex, healthcare users might abstain from using them.

See also health-specific implementation guidance in 8.2.1.

Other information

ISO/IEC 27002:2013, 13.2.1, applies.

Other health-specific information

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

13.2.2 Agreements on information transfer

Control

ISO/IEC 27002:2013, 13.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.2.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 13.2.2, applies.

Other health-specific information

As noted in 13.2.1, specific guidance on health information exchange policies can be found in ISO 22857. Though that International Standard explicitly references trans-border flow of personal health information (where borders in this context represent health jurisdictions, not necessarily national boundaries), much of its advice can be adapted, where necessary, to deal with exchange of data from one organization to another.

13.2.3 Electronic messaging

Control

ISO/IEC 27002:2013, 13.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 13.2.3, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations transmitting personal health information by electronic messaging should take steps to ensure its confidentiality and integrity. It is important to note that security of e-mail and instant messages containing personal health information may involve procedures for health personnel that cannot be imposed upon subjects of care and the public.

E-mail between health professionals which contains personal health information should be encrypted in transit. One approach to this involves the use of digital certificates. See Bibliography for a list of International Standards related to the use of digital certificates in health environments.

See also 18.1.4 for a discussion of consent prior to communication outside the organization.

Other information

ISO/IEC 27002:2013, 13.2.3, applies.

13.2.4 Confidentiality or non-disclosure agreements

Control

ISO/IEC 27002:2013, 13.2.4, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing personal health information shall have a confidentiality agreement in place that specifies the confidential nature of this information. The agreement shall be applicable to all personnel accessing health information.

Implementation guidance

ISO/IEC 27002:2013, 13.2.4, applies.

Health-specific implementation guidance

The agreement above should include reference to the penalties that are possible when a breach in the information security policy is identified.

Other information

ISO/IEC 27002:2013, 13.2.4, applies.

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

14.1.1 Information security requirements analysis and specification

Control

ISO/IEC 27002:2013, 14.1.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.1.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other health-specific information

ISO/TS 14441 contains a detailed set of functional privacy and security requirements for EHR systems.

14.1.1.1 Uniquely identifying subjects of care

Health-specific control

Health information systems processing personal health information:

a) shall ensure that each subject of care can be uniquely identified within the system;

b) shall be capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency.

Health-specific implementation guidance

The provision of emergency care and other situations in which adequate identification of subjects of care may not have been possible will inevitably create instances of multiple records for the same patient. Some capacity shall exist within every health information system to merge multiple instances of patient records into a single record. Such merging requires the greatest care and will therefore not only necessitate personnel trained in such merging, but may also require technical tools to better 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 is 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.

14.1.1.2 Output data validation

Health-specific control

Health information systems processing personal health information shall provide personally identifying information to assist health professionals in confirming that the electronic health record retrieved matches the subject of care under treatment.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, some additional important factors need to be considered. 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 retrieved. Matching a subject of care under treatment to an existing record can be a non-trivial task. Some systems enhance security by including photographic ID with each subject of care’s record. Such enhancements may 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 may 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 (e.g. page 3 of 5).

Other information

ISO/IEC 27002:2013, 14.1.1, applies.

14.1.2 Securing application services on public networks

Control

ISO/IEC 27002:2013, 14.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.1.2, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note the care that shall be taken in determining whether data involved in electronic commerce and online transactions contain personal health information. If they do, this information needs to be appropriately protected. Of special concern in healthcare are data related to billing, medical claims, invoice lines, requisitions, and other e-commerce data from which personal health information can be derived.

Other information

ISO/IEC 27002:2013, 14.1.2, applies.

14.1.3 Protecting application services transactions

Control

ISO/IEC 27002:2013, 14.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.1.3, applies.

Health-specific implementation guidance

See Health-specific implementation guidance in 14.1.2.

Other information

ISO/IEC 27002:2013, 14.1.3, applies.

14.1.3.1 Publicly available health information

Health-specific controls

Publicly available health information (as distinct from personal health information) should be archived.

The integrity of publicly available health information should be protected to prevent unauthorized modification.

The source (authorship) of publicly available health information should be stated and its integrity should be protected.

14.2 Security in development and support processes

Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.

14.2.1 Secure development policy

Control

ISO/IEC 27002:2013, 14.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 14.2.1, applies.

14.2.2 System change control procedures

Control

ISO/IEC 27002:2013, 14.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 14.2.2, applies.

14.2.3 Technical review of applications after operating platform changes

Control

ISO/IEC 27002:2013, 14.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 14.2.3, applies.

14.2.4 Restrictions on changes to software packages

Control

ISO/IEC 27002:2013, 14.2.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.4, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

14.2.5 Secure system engineering principles

Control

ISO/IEC 27002:2013, 14.2.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.5, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 14.2.5, applies.

14.2.6 Secure development environment

Control

ISO/IEC 27002:2013, 14.2.6, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.6, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

14.2.7 Outsourced development

Control

ISO/IEC 27002:2013, 14.2.7, applies.

Implementation guidance:

ISO/IEC 27002:2013, 14.2.7, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 14.2.7, applies.

14.2.8 System security testing

Control

ISO/IEC 27002:2013, 14.2.8, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.2.8, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

14.2.9 System acceptance testing

Control

ISO/IEC 27002:2013, 14.2.9, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing personal health information shall establish acceptance criteria for planned new information systems, upgrades and new versions. They shall carry out suitable tests of the system prior to acceptance.

Clinical users should be involved in the testing of clinically relevant system features.

Implementation guidance

ISO/IEC 27002:2013, 14.2.9, applies.

14.3 Test data

Objective: To ensure the protection of data used for testing.

14.3.1 Protection of test data

Control

ISO/IEC 27002:2013, 14.3.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 14.3.1, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should not use actual personal health information as test data.

Other information

ISO/IEC 27002:2013, 14.3.1, applies.

Other health-specific information

ISO/TS 14441 contains detailed guidance on conformance testing of EHR systems, including use of test data.

15 Supplier relationships

15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

15.1.1 Information security policy for supplier relationships

Control

ISO/IEC 27002:2013, 15.1.1, applies.

Health-specific control

In addition to implementing the control given by ISO/IEC 27002, organizations processing health information shall assess the risks associated with access by external parties to these systems or the data they contain, and then implement security controls that are appropriate to the identified level of risk and to the technologies employed.

Implementation guidance

ISO/IEC 27002:2013, 15.1.1, applies.

Other health-specific information

Risk assessment is essential for effective management of third-party access to systems containing health information, especially personal health information. The rights of subjects of care should be protected, even when an external 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.

Other information

ISO/IEC 27002:2013, 15.1.1, applies.

15.1.2 Addressing security within supplier agreements

Control

ISO/IEC 27002:2013, 15.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 15.1.2, applies.

Health-specific implementation guidance

Third-party service delivery management is greatly simplified when a formal agreement is adopted which specifies the minimum set of controls to be implemented.

Other information

ISO/IEC 27002:2013, 15.1.2, applies.

15.1.3 Information and communication technology supply chain

Control

ISO/IEC 27002:2013, 15.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 15.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 15.1.3, applies.

15.2 Supplier service delivery management

Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.

15.2.1 Monitoring and review of supplier services

Control

ISO/IEC 27002:2013, 15.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 15.2.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health. See also health-specific implementation guidance in 15.1.2.

15.2.2 Managing changes to supplier services

Control

ISO/IEC 27002:2013, 15.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 15.2.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health. See also health-specific implementation guidance in 15.1.2.

16 Information security incident management

16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.1 Responsibilities and procedures

Control

ISO/IEC 27002:2013, 16.1.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.1, applies.

Other information

ISO/IEC 27002:2013, 16.1.1, applies.

16.1.2 Reporting information security events

Control

ISO/IEC 27002:2013, 16.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.2, applies.

Health-specific controls

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should establish security incident management responsibilities and procedures in order:

a) to ensure effective and timely response to security incidents;

b) to ensure that there is an effective and prioritized escalation path for incidents, such that crisis management and business continuity management plans can be invoked in the right circumstances and at the right time;

c) to collect and preserve incident-related audit logs and other relevant evidence.

Information security incidents include corruption or unintentional disclosure of personal health information or the loss of availability of health information systems, where such a loss adversely affects patient care or contributes to adverse clinical events.

Organizations should inform the subject of care whenever personal health information has been unintentionally disclosed.

Organizations should inform the subject of care whenever lack of availability of health information systems may have adversely affected their care.

Health-specific implementation guidance

There is a tendency in health organizations to artificially separate information security incidents from other types of incident, both in handling and in reporting. In recognition of the fact that a break-in could have led to theft of IT hardware (leading to a confidentiality breach), or that a fire could have been set to disguise misuse of IT equipment, or that an identified misuse or erroneous use of the system could have had clinical consequences, an information security assessment should be made either on all such incidents or on a representative incident, to further evaluate the efficacy of established controls and of the risk assessment that lead to their implementation.

Other information

ISO/IEC 27002:2013, 16.1.2, applies.

Other health-specific information

In many jurisdictions, data breaches involving personally identifiable information shall, by law, be reported to the data subjects whose personal information was breached. Even in those jurisdictions where no such law exists for personally identifiable information in general, there may be laws requiring notification of patients where their personal health information is breached (e.g. four Canadian provinces have laws requiring notification of breaches of personal health information, despite having no similar breach notification law for other personally identifiable data).

Information security events may include patient safety incidents where data processing or data transfer played a role.

In some jurisdictions, patients have a right to be informed of any breach of their personal health information.

16.1.3 Reporting information security weaknesses

Control

ISO/IEC 27002:2013, 16.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 16.1.3, applies.

16.1.4 Assessment of and decision on information security events

Control

ISO/IEC 27002:2013, 16.1.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.4, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should assess whether the information security event involved personal health information.

16.1.5 Response to information security incidents

Control

ISO/IEC 27002:2013, 16.1.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.5, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 16.1.5, applies.

16.1.6 Learning from information security incidents

Control

ISO/IEC 27002:2013, 16.1.6, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.6, applies.

Other information

ISO/IEC 27002:2013, 16.1.6, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

16.1.7 Collection of evidence

Control

ISO/IEC 27002:2013, 16.1.7, applies.

Implementation guidance

ISO/IEC 27002:2013, 16.1.7, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information may need to consider the implications of collecting evidence for purposes of establishing medical malpractice and may also need to consider inter-jurisdictional requirements when health information systems are accessible across jurisdictional boundaries.

Other information

ISO/IEC 27002:2013, 16.1.7, applies.

17 Information security aspects of business continuity management

17.1 Information security continuity

Objective: Information security continuity should be embedded in the organization's business continuity management systems.

17.1.1 Planning information security continuity

Control

ISO/IEC 27002:2013, 17.1.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 17.1.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, the following considerations are important in healthcare environments. Business continuity management, which includes disaster recovery, is increasingly recognised as a requirement for health organizations and the priority it is accorded continues to grow. Reflecting the rigorous availability requirements in healthcare, a major effort ought to be invested in resilience and redundancy arrangements, not just for the technology itself, and but also for the cross-training of health personnel.

Business continuity planning in healthcare is especially challenging for the information security professional, as any plans will need to be suitably integrated with the organization's plans for handling power failures, implementing infection control and dealing with other clinical emergencies. Indeed, the invocation of any of these is likely to lead directly to the invocation of the business continuity management plan, if only to provide support additional to that normally available. However, recent incidents such as the SARS outbreak have shown that major incidents may cause a staff shortage, which may then severely limit the ability to successfully operate business continuity management plans.

Health organizations should ensure that their business continuity management planning includes health crisis management planning. Patient lives may depend upon access to patient data and it is essential that this be taken into account during planning. Catastrophes and force majeure crises that would disable IT systems in other industrial sectors are the very events that may 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.

Finally, health organizations should remain cognizant of the role that health information systems play in patient continuity of care. Such organizations should be prepared if/when IT systems fail.

Other information

ISO/IEC 27002:2013, 17.1.1, applies.

17.1.2 Implementing information security continuity

Control

ISO/IEC 27002:2013, 17.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 17.1.2, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, organizations processing personal health information should identify processes, systems and other relevant equipment that are vital in health care delivery.

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

Other information

ISO/IEC 27002:2013, 17.1.2, applies.

17.1.3 Verify, review and evaluate information security continuity

Control

ISO/IEC 27002:2013, 17.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 17.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 17.1.3, applies.

17.2 Redundancies

Objective: To ensure availability of information processing facilities.

17.2.1 Availability of information processing facilities

Control

ISO/IEC 27002:2013, 17.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 17.2.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 17.2.1, applies.

18 Compliance

18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

18.1.1 Identification of applicable legislation and contractual requirements

Control

ISO/IEC 27002:2013, 18.1.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.1.1, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, health organizations should put a compliance auditing programme in place that addresses the full life cycle of operations, not just of those processes that identify issues, but also of those that review outcomes and that decide on updates to the ISMS.

Health organizations' audit programmes should be formally structured to cover all elements of this International Standard, all areas of risk and all implemented controls, within a 12 month to 18 month cycle.

In the highly regulated and audited environment of many health organizations, the ISMF ought to 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 ISMF, internal auditing, controls assurance assessments and external audits, ought to be defined in a manner that allows each layer to draw confidence from all of the layers below it.

18.1.2 Intellectual property rights

Control

ISO/IEC 27002:2013, 18.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.1.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 18.1.2, applies.

18.1.3 Protection of records

Control

ISO/IEC 27002:2013, 18.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 18.1.3, applies.

18.1.4 Privacy and protection of personally identifiable information

Control

ISO/IEC 27002:2013, 18.1.4, applies.

Health-specific implementation guidance

In addition to following the guidance given by ISO/IEC 27002, organizations processing personal health information should manage informational consent of subjects of care.

Where possible, informational consent of subjects of care should be obtained before personal health information is e-mailed, faxed, communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organization.

Implementation guidance

ISO/IEC 27002:2013, 18.1.4, applies.

Health-specific implementation guidance

An example of legislation or regulation requiring informational consent from subjects of care is the Council of Europe Recommendation, R (97)5 On the Protection of Medical Data, Council of Europe, Strasbourg, 12 February 1997:

Before a genetic analysis is carried out, the data subject should be informed about the objectives of the analysis and the possibility of unexpected findings.

They should be informed of unexpected findings if:

a) not prohibited by domestic law

b) the person himself has asked for this information

c) the information is not likely to cause serious harm:

   1) to his/her health

   2) to his/her consanguine or uterine kin, to a member of his/her social family, or to a person who has a direct link with his/her genetic line

d) this information is of direct importance to him/her for treatment or prevention.

An example of a professional ethical guideline requiring patient consent is the World Health Association's Declaration of Helsinki regarding medical research on human subjects.

Other information

ISO/IEC 27002:2013, 18.1.4, applies.

Other health-specific information

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

18.1.5 Regulation of cryptographic controls

Control

ISO/IEC 27002:2013, 18.1.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.1.5, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

18.2 Information security reviews

Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

18.2.1 Independent review of information security

Control

ISO/IEC 27002:2013, 18.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.2.1, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 18.2.1, applies.

18.2.2 Compliance with security policies and standards

Control

ISO/IEC 27002:2013, 18.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.2.2, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 18.2.2, applies.

18.2.3 Technical compliance review

Control

ISO/IEC 27002:2013, 18.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 18.2.3, applies.

Health-specific implementation guidance

Special attention is drawn to compliance for the purpose of technical interoperability, as large-scale health information systems typically consist of many interoperating systems.

Other information

ISO/IEC 27002:2013, 18.2.3, applies.

Annex A
(informative)

Threats to health information security

Threats to the confidentiality, integrity and availability of health information assets include all of the following:

a) Masquerade by insiders (including masquerade by health professionals and support staff). Masquerade by insiders consists of system use by those who make use of accounts that are not their own. As such, it constitutes a breakdown in secure user authentication. Many cases of masquerade by insiders are committed simply because it makes it easier for people to do their work. For example, when one health professional may replace another at a workstation and continues to work on an already active subject of care record, there is a strong temptation to skip the inconvenience of the first user logging out and the second user logging in. Nevertheless, masquerade by insiders is also the source of serious breaches in confidentiality. Indeed, the majority of breaches of confidentiality are committed by organizational insiders. Masquerade by insiders can also be carried out with the intention to cover up cases where harm has been caused.

b) Masquerade by service providers (including contracted maintenance personnel, such as system software engineers, hardware repair personnel and others who may have a pro-forma legitimate reason to access systems and data). Masquerade by service providers consists of contracted personnel using their privileged access to systems (such as during on-site testing and repair of malfunctioning equipment) to gain unauthorised access to data. As such, it is a breach of, or failure to properly provide for, secure outsourcing arrangements. Though rarer than masquerade by insiders, masquerade by service providers can also be the source of serious breaches in personal health information confidentiality.

c) Masquerade by outsiders (including hackers). Masquerade by outsiders occurs when unauthorised third parties gain access to system data or resources, either by impersonating an authorised user or by fraudulently becoming an authorised user (for example, through so-called “social engineering”). In addition to hackers, masquerade by outsiders is also committed by journalists, private investigators, and “hacktivists” (hackers who work on behalf of, or in sympathy with, political pressure groups). Masquerade by outsiders constitutes a failure of one or more of the following security controls:

   1) user identification;

   2) user authentication;

   3) origin authentication;

   4) access control and privilege management.

d) Unauthorised use of a health information application. It can be surprisingly easy to obtain unauthorised access to a health information application (for example, by a subject of care walking up to an unattended workstation in a physician care office and browsing the screen). Authorized users can also perform unauthorised actions, such as maliciously altering data. In the UK, Dr. Harold Shipman attempted to hide the notorious murder of scores of his patients by altering records on his computer system.

   The critical importance of correctly identifying subjects of care and correctly matching them to their health records leads health organizations to collect detailed identifying information on patients treated. This identifying information is of great potential value to those who would use it to commit identity theft and so should be rigorously protected.

In general, unauthorised use of health information applications constitutes a failure of one or more of the following:

1) workgroup access control (e.g. by allowing a user to access the records of subjects of care with whom the user has no legitimate relationship);

2) accountability and audit control (e.g. by allowing inappropriate user actions to go unnoticed);

3) personnel security (e.g. by providing inadequate training to users or making clear that their access to records is subject to audit and review).

e) Introduction of damaging or disruptive software (including viruses, worms, and other "malware"). Most IT security incidents involve computer viruses. Introduction of damaging or disruptive software constitutes a failure in anti-virus protection or in software change control. While typically within the remit of network sysops, the proliferation of email worms and viruses as well as exploitation by hackers of weaknesses in server software have combined to greatly complicate measures taken to prevent the introduction of damaging or disruptive software.

f) Misuse of system resources.

This threat includes users using health information systems and services for personal work, users downloading non-work related information from the Internet onto computers intended solely to support health information systems, users setting up databases or other applications for non-work related matters, or users degrading the availability of health information system by, for example, using network bandwidth to download streaming video or audio for personal use. Such misuse constitutes a failure to enforce acceptable use agreements or to educate users about the importance of maintaining the integrity and availability of health information resources.

g) Communications infiltration.

Communications infiltration of electronic communications occurs when an individual (a hacker, for example) tampers with the normal flow of data across a network. The most common result is a denial of service attack (in which servers or network resources are effectively taken off-line), but other forms of communication infiltration are possible (such as a replay attack, in which a valid but out-of-date message is retransmitted in a way that makes it appear current). Communications infiltration constitutes a failure of intrusion detection and/or network access controls and/or risk analysis (specifically vulnerability analysis) and/or system architecture (which needs to be designed with defence against denial-of-service attacks).

h) Communications interception.

If not encrypted during transmission, the confidentiality of information contained in a message can be abrogated by intercepting the communication. This is simpler than it sounds, as anyone on local area network can potentially install a so-called "packet sniffer" on their workstation and monitor much of the network traffic on their local area network, including reading emails during transmission. Hacker tools are readily available to automate and simplify much of this process. Communications interception constitutes a failure in secure communications.

i) Repudiation.

This threat includes users denying that they sent a message (repudiation of origin) and users denying that they received a message (repudiation of receipt). Unambiguously establishing whether personal health information flowed from one health professional to another can be an essential feature of investigations into medical malpractice. Repudiation can constitute a failure to apply controls such as digital signatures on e-prescriptions (an example of repudiation of origin) or controls, such as read receipts on email messages (an example of repudiation of receipt).

j) Connection failure (including failures of health information networks).

All networks are subject to periodic service outages. Quality of service is a major factor in the provisioning of network services in healthcare. Connection failure can also result from misdirection

of network services (for example, malicious alteration of routing tables that cause network traffic to be diverted). Connection failures can facilitate the disclosure of confidential information by forcing users to send messages by a less secure mechanism, such as through fax or over the Internet.

k) Embedding of malicious code.

This threat includes email viruses and hostile mobile code. While in no way unique to health information systems, the increasing use of wireless and mobile technologies by health professionals increases this threat's potential for damage. Embedding of malicious code constitutes a failure to effectively apply anti-virus software controls or intrusion prevention controls.

l) Accidental misrouting.

This threat includes the possibility that information might be delivered to an incorrect address when it is being sent over a network. Accidental misrouting could constitute a failure in user education or a failure to maintain the integrity of directories of health professionals (or both).

m) Technical failure of the host, storage facility, or network infrastructure.

These threats include hardware failures, network failures, or failures in data storage facilities. Such failures typically constitute a failure of one or more of the operations management controls listed in ISO/IEC 27002:2013, Clause 10. While in no way unique to health information systems, the loss of availability of such systems can have life-threatening consequences for patients.

n) Environmental support failure (including power failures and disruptions of service arising from natural or man-made disasters).

Health information systems can be critically needed during natural disasters and other events that can be life-threatening to large numbers of people. These same disasters can wreck havoc on the environmental support systems needed to maintain operations. A proper threat and risk assessment of health information will include an assessment of how critical such systems are in times of natural disaster and how robust their operations will be under such disaster scenarios.

o) System or network software failure.

Denial of service attacks are greatly facilitated by weaknesses in or misconfiguration of operating system or network operating system software. System or network software failure constitutes a failure in software integrity checking, system testing, or software maintenance controls.

p) Application software failure (e.g. of a health information application).

Failures in application software can be exploited in a denial of service attack and can also be used to compromise the confidentiality of protected data. Application software failure constitutes a failure in software testing, software change controls, or software integrity checking.

q) Operations error.

Operator error accounts for a small but significant percentage of unintentional disclosures of confidential information and a large proportion of unintentional dispositions of data. Operator error constitutes a failure in one or more of the following:

1) operations controls;

2) personnel security (including effective training);

3) disaster recovery (including data backup and restoration).

r) Maintenance error.

Maintenance errors are mistakes by those responsible for maintaining systems hardware and software. Maintenance errors can be committed by staff members, as well as by third party employees contracted to perform maintenance duties. Such errors can, in turn, endanger the confidentiality of protected data. Misconfiguration of software during installation is a common

cause of vulnerabilities later exploited by hackers. Maintenance errors constitute a failure in hardware maintenance controls, software maintenance controls, software change controls, or some combination of the above.

s) User error.

Error by users can, for example, result in confidential information being sent to the wrong recipient. User errors can sometimes constitute a failure in

1) user controls (including user interfaces designed with security in mind), and

2) personnel security (including training).

t) Staff shortage.

The threat of staff shortage includes the possibility of the absence of key personnel and the difficulty of replacing them. Vulnerability to this threat depends on the extent to which shortage of staff would affect the business processes. In healthcare, an epidemic that greatly increases the demand for timely access to health information may also create a staff shortage that jeopardizes the availability of such systems. A failure of this kind constitutes a failure in business continuity management (see ISO/IEC 27002:2013, Clause 14).

u) Theft by insiders (including theft of equipment or data).

Insiders typically have greater access to confidential information than outsiders and are therefore in a favourable position to steal the information in order to sell it or to disclose it to others. While comparatively rare, the threat of theft of personal health information by insiders increases with the fame or notoriety of the data subject (e.g. a celebrity or head of state) and decreases with the potential severity of punitive consequences (e.g. the loss by a physician of her license to practice). Theft by insiders constitutes a failure of one of many possible controls, including controls on hardcopy output, documents, or media, physical security or physical protection of equipment.

v) Theft by outsiders (including theft of equipment or data).

Theft by outsiders of data and equipment is a serious problem in some hospitals. Theft may result in breaches of confidentiality, either because confidential data resides on a server or laptop computer that is stolen or else because the data itself is the target of the theft. Theft by outsiders may constitute a failure in one of many controls, including mobile computing controls, secure media transport, incident handling, compliance checks, or physical theft protection.

w) Wilful damage by insiders.

Wilful damage by insiders includes acts of vandalism and other cases where physical damage is caused to IT systems or their supporting environment by people who have been granted access. The users of health information systems are typically dedicated health professionals and wilful damage is rare. Wilful damage by insiders constitutes a failure of human resources security (see ISO/IEC 27002:2013, Clause 8).

x) Wilful damage by outsiders.

The threat of wilful damage by outsiders includes acts of vandalism and other cases where physical damage is caused to IT systems or their supporting environment by people who have not been granted access to such systems. While in most industrial sectors, failures of this kind constitute a failure to effective apply physical security controls, access by subjects of care and their friends and relatives to operational areas of hospitals, clinics and other health organizations make such threats much more difficult to prevent than in most other operational environments. The security controls in ISO/IEC 27002:2013, Clause 9 need to be carefully selected and applied to minimise such threats.

y) Terrorism.

The threat of terrorism includes acts by extremist groups wishing to damage or disrupt the work of health organisations, or to harm health professionals, or to disrupt the operations of

health information systems. While no such large-scale attacks have occurred yet, planners need to consider the threat of terrorism, especially when large-scale health information systems are designed, since an attack on such systems could increase the effectiveness of bioterrorist and other attacks that cause a health-related crisis.

Annex B
(informative)

Practical action plan for implementing ISO/IEC 27002 in healthcare

B.1 Taxonomy of the ISO/IEC 27001 and ISO/IEC 27002 International Standards

Implementers of ISO/IEC 27002 in health environments will find that most of its control objectives will apply in almost all situations. However, users of the standard in healthcare need also to recognize situations in which additional control objectives may be needed. This is often the case where clinical processes intersect with specialist devices such as scanners, infusion machines, etc., even if the security controls only relate to maintenance of device data integrity. Different jurisdictions will also have different legal frameworks that may change the required scope of compliance activities.

ISO/IEC 27001 introduces the concept of an information security management system (ISMS) and describes the need for this detailed framework of controls when an effort is made to meet the security objectives revealed as relevant by risk assessment. International experience and recognised information security best practice principles indicate that on-going compliance with ISO/IEC 27002 can best be ensured by the implementation of a management system as depicted in Figure B.1.

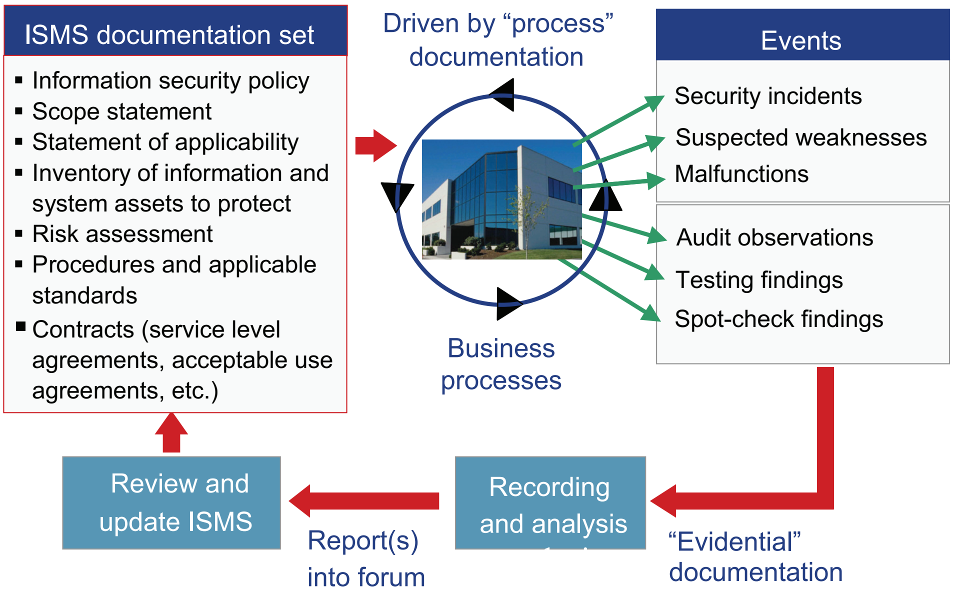

Figure B.1 — Information Security Management System

Health organizations should, where possible, integrate their ISMS with the information governance processes described below, and take account of the guidance given in the following clauses.

A common mistake made, especially by public health organizations where there is typically no central requirement for formal accreditation or certification, is to describe compliance with ISO/IEC 27002 as being a matter of adoption of a checklist. To be truly compliant, organizations need to be able to demonstrate an operational ISMS in which there are appropriate compliance auditing processes. This compliance fits well with the regulatory frameworks under which health organizations typically operate.

B.2 Management commitment to implementing ISO/IEC 27002

It is important that a health organization have the evident support of management before trying to achieve compliance with ISO/IEC 27002. As management's active involvement and support are essential for success, that involvement should include written and verbal statements of commitment to the importance of health information security and recognition of its benefits. Risk assessment brings with it the potential for discovering serious risks that in turn may require substantial changes to existing processes in order for these risks to be mitigated. The personal willingness of management to subject themselves and the organization to changes in processes and to be pioneers of those changes needs to be clearly shown.

B.3 Establishing, operating, maintaining and improving the ISMS

The four subclauses that follow (B.4 to B.7) provide guidance on establishing and then operating an ISMS in a health environment. This requires pursuing a cycle of activities, as illustrated in Figure B.2.

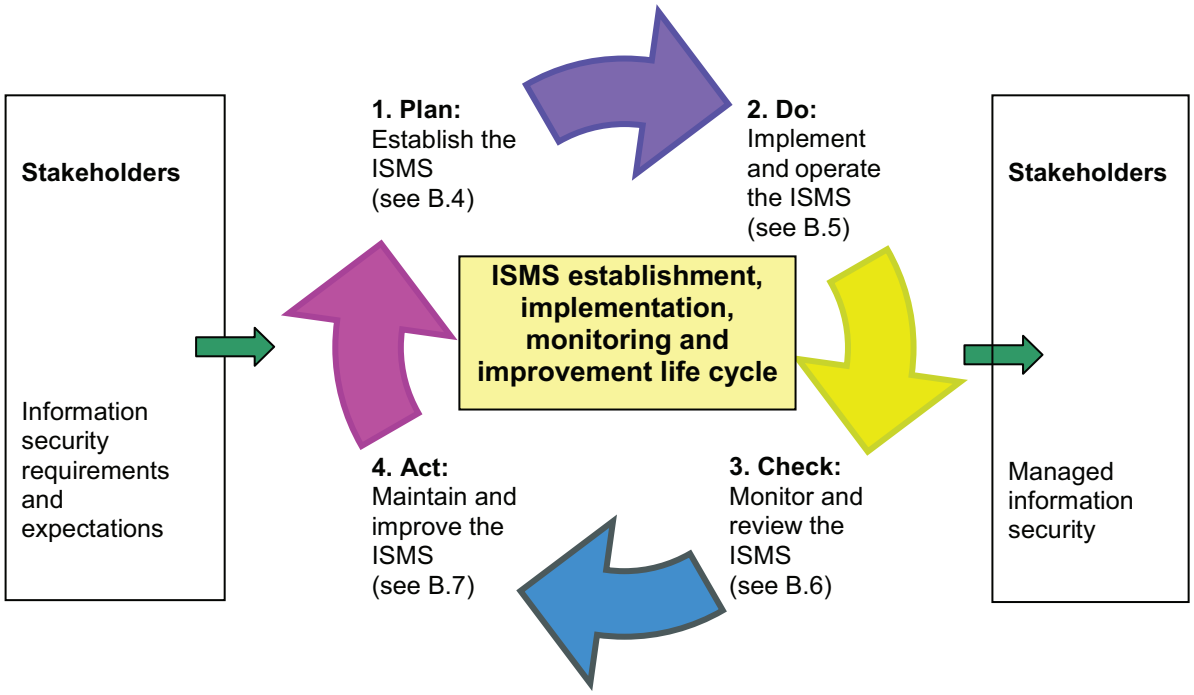

Figure B.2 — ISMS process overview

B.4 Planning: establishing the ISMS

B.4.1 Selecting and defining a compliance scope

B.4.1.1 General

In theory, ISO/IEC 27002 can be applied to whole organizations. However, experience from implementations in the UK and elsewhere has shown that very large units struggle to complete the work involved and to deliver the necessary level of compliance in one attempt.

In healthcare, the extensive interdependency of functions makes scope definition a challenge. For this reason, it is all the more important to get it right. Compliance scopes that cover no more than two to three healthcare sites or approximately 50 staff or approximately 10 processes have been found to work very well. For this reason, it is best for primary care practices, clinics, home visit teams, hospital

specialties and directorates, etc., to all make effective scopes. An incremental and iterative process is then typically followed to achieve total coverage and full benefit. The prospects for achieving such results ought not to be undermined by the selection of an overly broad compliance scope. However, where third party providers of IT services are employed, "Management of IT Services Delivery" has been widely adopted as a scope for compliance, with considerable success.

In health organizations as elsewhere, activity in recent years has successfully moved information security from being a technical or "back office" function to being a prominent corporate responsibility.

B.4.1.2 Criteria for defining the compliance scope

To appropriately balance the "deliverability" of compliance with corporate benefit, many public sector organizations, including health organizations, have defined an initial scope of "Secure Delivery of IT Services". Though related more directly to infrastructure than to business processes, this scope confers real corporate benefits insofar as it accomplishes critical tasks, including securing the infrastructure as a whole, stimulating the implementation of any needed updates to the corporate security processes, and improving identity management, information security awareness and business continuity management. Typically, in many of these areas, corporate benefits over and above the chosen scope will result.

It is essential, therefore, that criteria be used to define the scope. The criteria cover such topics as the following:

a) the degree of visibility sought;

b) the balance of business and technical involvement intended;

c) the degree of local or centralized control sought;

d) the extent of manageability that the scope will introduce.

B.4.1.3 Potential summary level gap analysis while defining the compliance scope

Before making the final selection of a scope, it may be appropriate to undertake a summary level gap analysis on a sampling basis to get a "feel" for how much work different areas may involve before making the final selection. Whether an "easy" or "hard" area is chosen is a matter for the organization to decide, although logically, commensurately more corporate benefit is to be gained from taking on the "hard" aspects of the scope.

B.4.1.4 Controlled involvement/inclusion of third parties

Another typical area in which errors are made is the interpretation of scope. Scope includes the services delivered by third parties and the delivery of required supporting processes but not a determination of how those supporting processes are delivered.

B.4.1.5 Service level agreements (SLAs) and contracts help establish the scope

SLAs and contracts can also assist in defining scope, in as much as these instruments effectively define the scope boundary. Even if they do not do so clearly in some cases, reviewing them will still prove worthwhile for clarifying likely priorities for improvement.

B.4.1.6 Producing and disseminating the scope statement

A formal scope statement needs to be produced, especially if certification is sought under ISO/IEC 27001. The statement ought to be publicised widely within the organization. It is essential that the scope statement define the boundary of the compliance activity in terms of people, processes, places, platforms and applications.

In the case of health organizations, this statement ought to be publicised widely, reviewed and adopted by the organization's information, clinical and corporate governance groups. Indeed, some health

organizations are known to have sought comments on the statement from clinicians' professional regulatory bodies, which may be aware of other organizations pursuing compliance or certification.

See 6.1.1 for minimum requirements relating to scope statements.

B.4.2 Gap analysis

Once the scope has been selected, the next stage of the planning process is a gap analysis in which a high-level assessment of compliance is undertaken. Best practice has shown that the focus of this analysis needs to be on organizational responsibility, implementation, and documentation of security practices as well as the evidence used to support the analysis. This is consistent with health practices where appropriate skills, records and procedures are all important.

A common failure of such analyses is not obtaining comparative viewpoints and corroboration: the analyst risks obtaining comments that could merely reflect the aspirations of certain individuals rather than a coherent view of current practice. Time needs to be invested in interviewing health professionals and managers to obtain a well-rounded view.

The purpose of gap analysis is to provide initial guidance on required improvements, pending detailed evaluation of the risk assessment and risk treatment (see B.4.4). Also, gap analysis can suggest an initial priority rating for such improvements.

B.4.3 Establishing or enhancing a health information security forum

At the heart of the ISMS, an appropriate information security management forum (ISMF) should be established to oversee and direct information security. What constitutes "appropriate" in this context varies among organizations and will also vary across the spectrum of healthcare.

Structuring the forum will be challenging, with many stakeholders' views to be accommodated and many regulatory obligations to be met. While the functions of the ISMF cannot be devolved or dispersed without losing effectiveness, neither should creation of the ISMF be taken as a mandate to create "yet another committee". It is usually better to extend the focus of an existing committee, such as one that addresses risks or that undertakes information governance. Membership will need to encompass the full range of information assurance and information governance functions, as well as representatives of the different user communities and representatives of the key support functions. Representatives of Internal Audit and Human Resources are also typically present.

The organizations' (virtual or actual) Information Security Officer should, among other duties, report to the forum and provide it with secretariat services, and should also be responsible for collating, publishing and commenting on the reports received by Forum members.

The central nature of information security within information governance makes the positioning of the ISMF within the information governance structure a sensible arrangement, but only if the latter group is, in turn, linked to the clinical governance structure. Clinical governance deals with patient safety issues and these are often closely related to the health information security issues to which information governance must attend. Taking an information governance approach underscores the critical nature of information security and also allows an integrated process, with risk analysis input, that directly feeds clinical governance. The removal of the "silo" mentality separating information security, data protection, freedom of information, etc., eliminates duplicated costs and enhances process integrity.

B.4.4 Assessing risks to health information

Risk assessment is the mechanism by which the controls framework is identified that delivers the ISO/IEC 27002 control objectives. This process is well documented in ISO/IEC 27005.

A risk is composed of a causal relationship between several risk sources. Figure B.3 shows the relationship between risks and risk sources in ISO/IEC 18028-4, making it clear that a risk value is determined from the surrounding asset values, threats, and vulnerabilities.

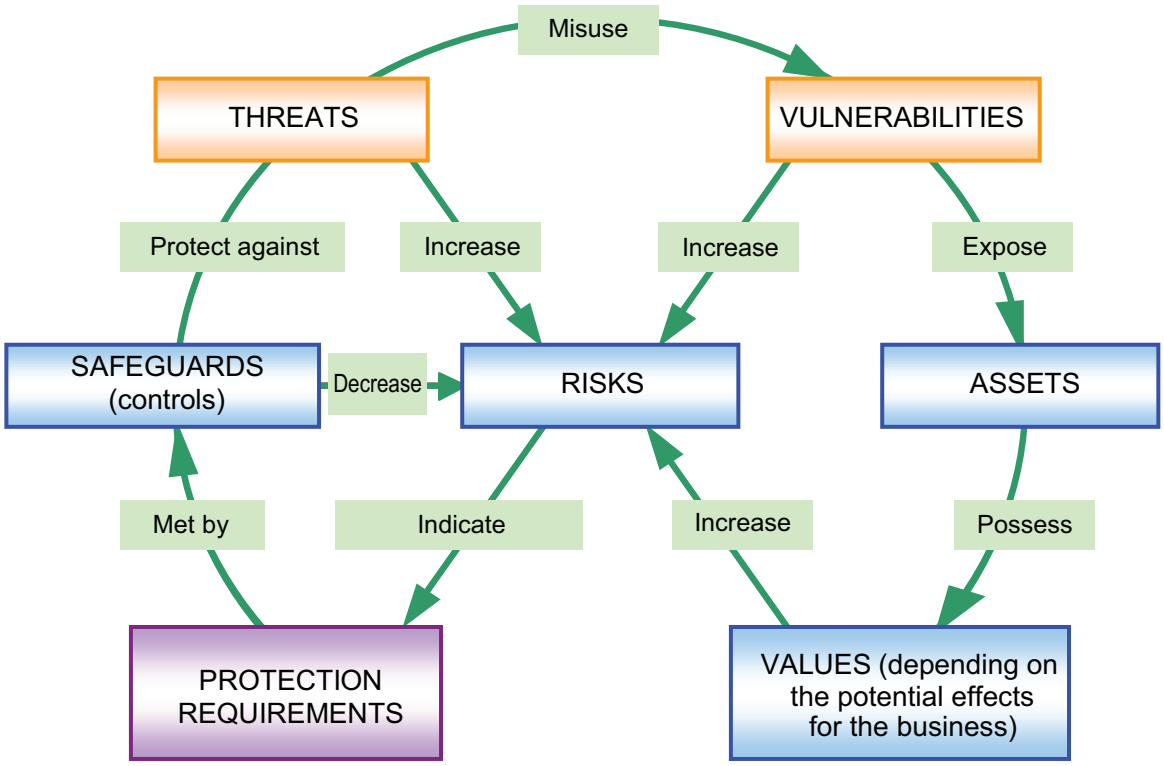

Figure B.3 — Relationship between risks and risk sources in a simplified risk model

Both ISO/IEC 27001 and ISO/IEC 27005 define the components of risk analysis and management as follows:

a) identification of business assets, threats and vulnerabilities;

b) business impact assessment;

c) threat likelihood and vulnerability assessment;

d) determination of risk levels;

e) identification of recommended security controls;

f) comparison with existing controls, allowing identification of areas of residual risk;

g) options for risk treatment, including, direct management, risk acceptance, avoidance, managed transference, etc.;

h) risk assessment and risk treatment plans;

i) mapping of decisions taken against the list of ISO/IEC 27002 controls.

All of these are applicable to healthcare, although “business impact assessment” clearly needs to include many different health professions. Information security risk assessments performed by health organizations would benefit from following this model.

In addition to the list above, it is important to also establish an understanding of the dependency of business processes upon IT services, hardware, software, media and locations. Without this understanding following the business impact analysis, understanding the failure scenarios that are relevant will be nearly impossible. In light of the severe impacts possible in health organizations, understanding these dependencies is essential.

There are a number of special considerations in the health arena that are worthy of discussion.

a) High levels of risk: Healthcare carries relatively high risks, especially in areas such as laboratories, emergency departments and operating theatres. A finding of low risk in the health information activities that support such areas ought therefore to be questioned, although the trap of assuming that every health information activity directly relates to care delivery would be equally wrong.

b) Qualitative as well as quantitative risk evaluation: Information security risk assessments in healthcare ought to consider qualitative as well as quantitative factors. Financial losses should not be the primary consideration but may be taken into account where there is evidence of large sums being paid for negligence. Careful design of valuation guidelines relevant to healthcare will be required, guidelines recognising the importance of patient safety, uninterrupted availability of emergency services, professional accreditation and clinical regulation.

c) Diverse inputs required: Risk analysis cannot typically be delivered by any single individual, except to the extent that the individual may give their personal viewpoints. Rather, it is an activity designed to seek consensus, so that all viewpoints are collected and indeed respected. Effective information security risk assessment in healthcare requires the availability of the following skills and knowledge:

   — clinical and nursing process knowledge, including care protocols and pathways;

   — knowledge of the formats of clinical data and the capability for the misuse of this data;

   — knowledge of external environment factors that could exacerbate or moderate any or all of the levels of the risk components described previously;

   — information on IT and medical device attributes and performance/failure characteristics;

   — knowledge of incident histories and actual case impact scenarios;

   — detailed knowledge of systems architectures;

   — familiarity with change management programmes that would change any or all of the risk component levels.

   When assessing risks, actual past incidents are by default realistic but they may not be the worst case. Defining worst cases may well require specialist input. Health professionals are likely to benefit from the input of IT staff who will be able to identify failure modes and scenarios requiring assessment.

d) Compliance obligations: Since healthcare is a sector with significant compliance obligations (both legal and professional) and risk management responsibilities, an output that maps together related risk assessments, performed by different disciplines or functional groups, ought to be considered as an aid to good information governance and also to help ensure the integrity of individual risk assessments.

B.4.4 Risk management

Risk assessment is intended as a means to an end. It should not an end in itself, but it often ends up that way. This is especially true in environments with resource constraints, such as those found in many health organizations. Risk management responds to the risk assessment by identifying which controls need to be strengthened, which controls are already effectively in place and which additional controls the organization needs to implement in order to reduce the residual level of risk to an acceptable level.

The interconnection of health information systems makes risk management in healthcare especially challenging, as few health organizations can act as if their systems were isolated islands of information. Risk assessment in healthcare frequently raises questions about information custodianship, ownership, and responsibility. Effective risk management must ensure the alignment of responsibility for information security with the authority to make risk management decisions.

To clearly distinguish the risk management process as a whole from the act of managing identified risks, Australian and New Zealand standard AS/NZ 4360 introduced the concept of "risk treatment." This concept has subsequently been adopted by ISO/IEC 27001.

The label "risk treatment" highlights the activity of reducing risk to acceptable levels (recognising that sufficient resources will never be available to allow even a try at complete risk avoidance). Risk treatment is particularly apposite for health organizations, bringing with it as it does the concepts of treat, transfer, or tolerate in relation to risks.

The definition of what is acceptable is and should remain, individual to the organization and its personnel. It should reflect the organization's appetite for risk and should be used to ensure that spending on information security improvement is justified and represents a demonstrably good use of scarce financial resources. Health organizations need to define and document their criteria for the acceptance of risks. The health-specific factor to be taken into account includes the following:

a) health sector, industry, or organizational standards;

b) clinical priorities;

c) reactions of subjects of care.

Taken together with healthcare-independent factors typically considered in risk treatment, these factors will yield a cost benefit assessment that can underpin the necessary business case for seeking funding.

A decision taken, usually by the ISMF, to not implement a particular control may be entirely valid but ought to be formally recorded for periodic review and reassessment. Health organizations should document accepted risks.

The process above should include an agreement about when (although it is acceptable for it to be "never") the identified risk will be addressed by the implementation of the control(s). Plans for future implementations should be reflected in the organization's Security Improvement Plan.

B.4.5 Security improvement planning

Responsibility for the security improvement plan should be taken, on behalf the ISMF, by the organization's information security officer, data protection officer or risk manager, or by a similarly responsible officer of the organization.

Often formatted as a Gantt chart, the plan should be made available to clinical and other staff, as the plan is typically not a confidential document. Indeed, it can often be useful in demonstrating progress and process improvement.

The plan will be most effective in minimising interruptions to operations if it integrates information security improvements with planned changes in IT facilities and healthcare service provision. It also needs to recognise known periods of unusual healthcare activity such as the influx of a new batch of interns or trainees.

B.4.6 Statement of applicability

A statement of Applicability can be seen as an executive summary of the state of information security in the organization, of the organisation's interpretation of security requirements and of its strategy for implementing security solutions. Maintained by the information security officer or similar officer on behalf of the ISMF, this International Standard should be provided to those responsible for the clinical and corporate governance functions to form a key part of the governance documentation set. Its format is also typically suitable for use as an assessment or evidence tool in support of external auditing, clinical assurance and other regulatory inspections.

B.4.7 ISMS document set

The ISMS model shown in Figure B.1 above lists the documentation required. The essential documents are

— information security policy of the organization,

— scope statement,

— statement of applicability,

— inventory of information assets and system assets to be protected,

— risk assessment plans and reports,

— procedures and standards agreed upon, and

— contractual agreements (including service level agreements and acceptable use agreements).

In addition, the operation of the ISMF and its success in meeting clinical needs and priorities can be materially enabled if these priorities are documented by the clinical and corporate governance functions and then held by the ISMF as a part of the documentation set. This document then provides backup material in support of risk acceptance decisions taken by the ISMF.

B.4.8 Potential for facilitation by the use of tools

The process of ISO/IEC 27002 compliance involves a range of steps that generate a significant quantity of information and documentation. However, health organizations exist in a dynamic environment in which risks change and new controls are implemented. The overall integrity of this information and documentation therefore needs to be maintained.

Furthermore, the staged, compounding, extending and iterative nature of the processes involved means that the information is repeatedly manipulated and reused in multiple processes, with the results of a later process often requiring amendments to be made in an earlier process. Finally, decisions will typically be taken in the light of a range of factors that will require considerable cross-referencing.

Health organizations ought to consider adopting tools to support their ISO/IEC 27002 compliance. Although database tools are by no means mandatory, evidence has shown that they provide significant benefits. There are a wide range of tools available, at a range of costs, from the simple and cheap to the extensive and more expensive. Health organizations, when considering the adoption of tools, should seek out evidence of successful use by others and should consider carefully the associated training and maintenance costs, although these are unlikely to be major.

National health organizations will presumably want to maximise compliance while minimising costs. Clearly, it is unnecessary for hundreds of hospitals to do essentially the same risk assessments. To address this problem, the UK National Health Service, for example, developed a toolkit in which generic risk models of typical health environments had been captured. Local use of the tool thereafter focuses upon creating a customized solution consistent with the local situation while still maintaining compliance with a centrally defined model. A similar approach could also be taken to the ISO/IEC 27002 process steps.

Tool support to the ISO/IEC 27002 process should cover the following:

a) scoping and scope statement production (B.4.1);

b) gap analysis and gap analysis reporting (B.4.2);

c) asset definition and asset inventory reporting;

d) secure improvement planning, reporting and implementation status recording (B.4.6);

e) Statement of Applicability recording and reporting (B.4.7);

f) security resource definition and reporting.

More advanced tools additionally provide additional features such as asset valuation tools, dependency modelling support, countermeasure libraries, security documentation support, auditing support, "What If?" functionality and graphical reports.

B.4.9 Summary

Figure B.4 summarizes the steps in establishing an ISMS.

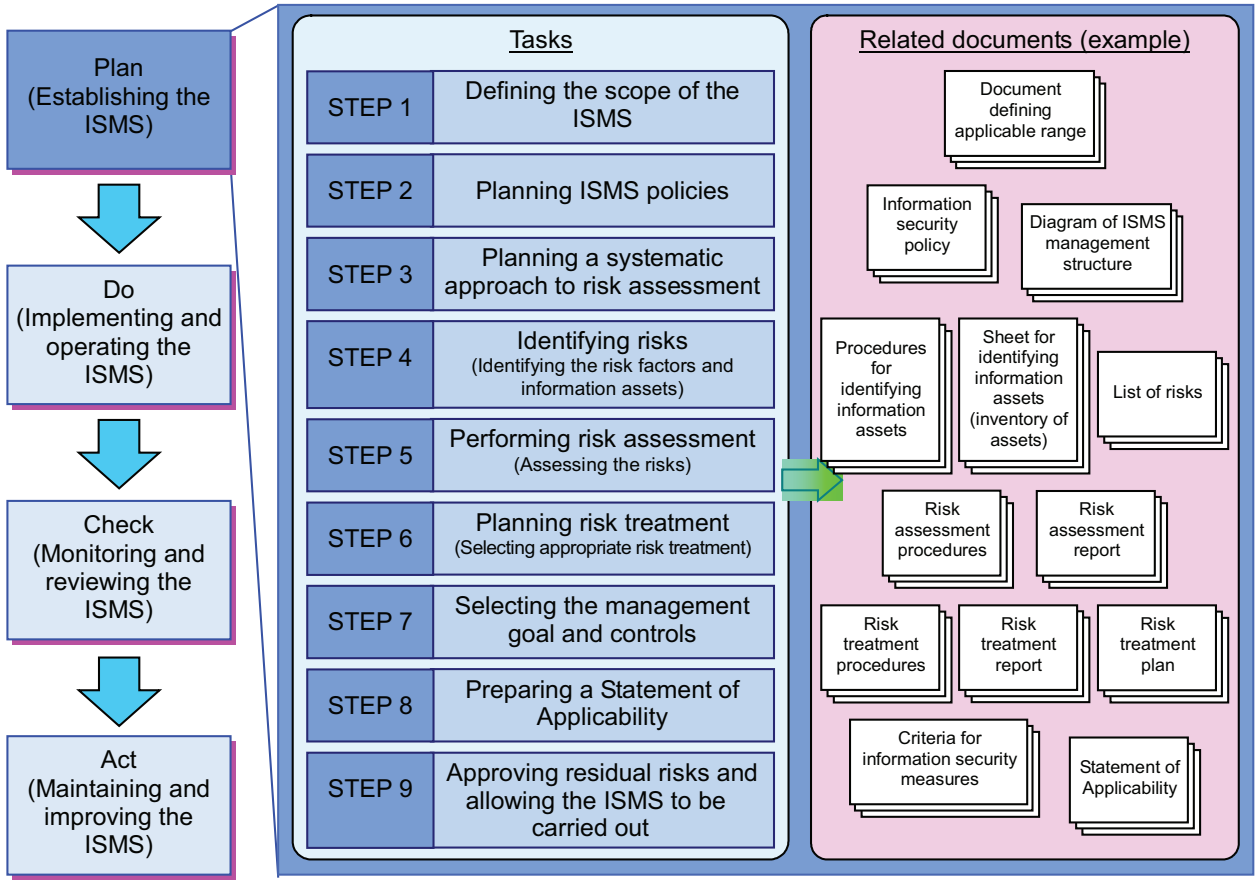

Figure B.4 — Tasks and related documents for establishing the ISMS

B.5 Doing: implementing and operating the ISMS

Implementing the ISMS involves several steps:

a) Creating a risk treatment plan: Once risks have been identified through a risk analysis, these risks should be examined and either accepted by senior management or mitigated where the risk is deemed unacceptable. A risk treatment plan clarifies the activities that need to be carried out to reduce unacceptable risks. It includes a plan for implementing the security controls chosen (based on the results of the risk assessment) to reduce or mitigate these unacceptable risks. The ISMF is responsible for ensuring that this plan is carried out. Ideally, a risk treatment plan will include schedules, priorities, and detailed work plans, and will also allocate responsibilities for implementing security controls. In healthcare, approving such plans can involve both information governance and clinical governance functions.

b) Allocating resources: An essential role of management is to provide the necessary resources (people, systems and funding) to ensure the security of health information assets.

c) Selecting and implementing security controls: Clause 5 of this International Standard reviews each of the security control areas of ISO/IEC 27002 and provides advice and guidance on the appropriate selection of security controls in a health environment.

d) Training and educating: 7.2.2 discusses the requirements for training and education for all staff, contractors, health professional and others who access health information systems and personal health information.

e) Managing operations: Competent ongoing operation of the ISMS is essential if the confidentiality, integrity and availability of health information and information systems is to be maintained. Clause 12 discusses health-related aspects of operations management.

f) Managing resources: Effective information security can be expensive and competent human resources scarce. Effective prioritization by the ISMF and careful management of people and resources are needed to ensure effective ongoing operations.

g) Managing security incidents: To minimize the consequences of a security incident, it is important that the incident be detected appropriately and that corrective action be taken. Procedure manuals for dealing with security incidents need to be prepared and regularly reviewed. It is especially important to define responsibilities and action steps in the initial phase of response, as events can unfold quickly and the critical nature of health information systems leaves little time for reflection as a security incident unfolds. Clear reporting procedures for security incidents are also essential so that the trust of healthcare stakeholders is maintained and that those responsible for corporate and clinical governance are apprised of significant events and their consequences. Clause 16 contains a detailed discussion of security incident management.

The task involved in implementing and operating the ISMS and the related documents produced are summarized in Figure B.5.

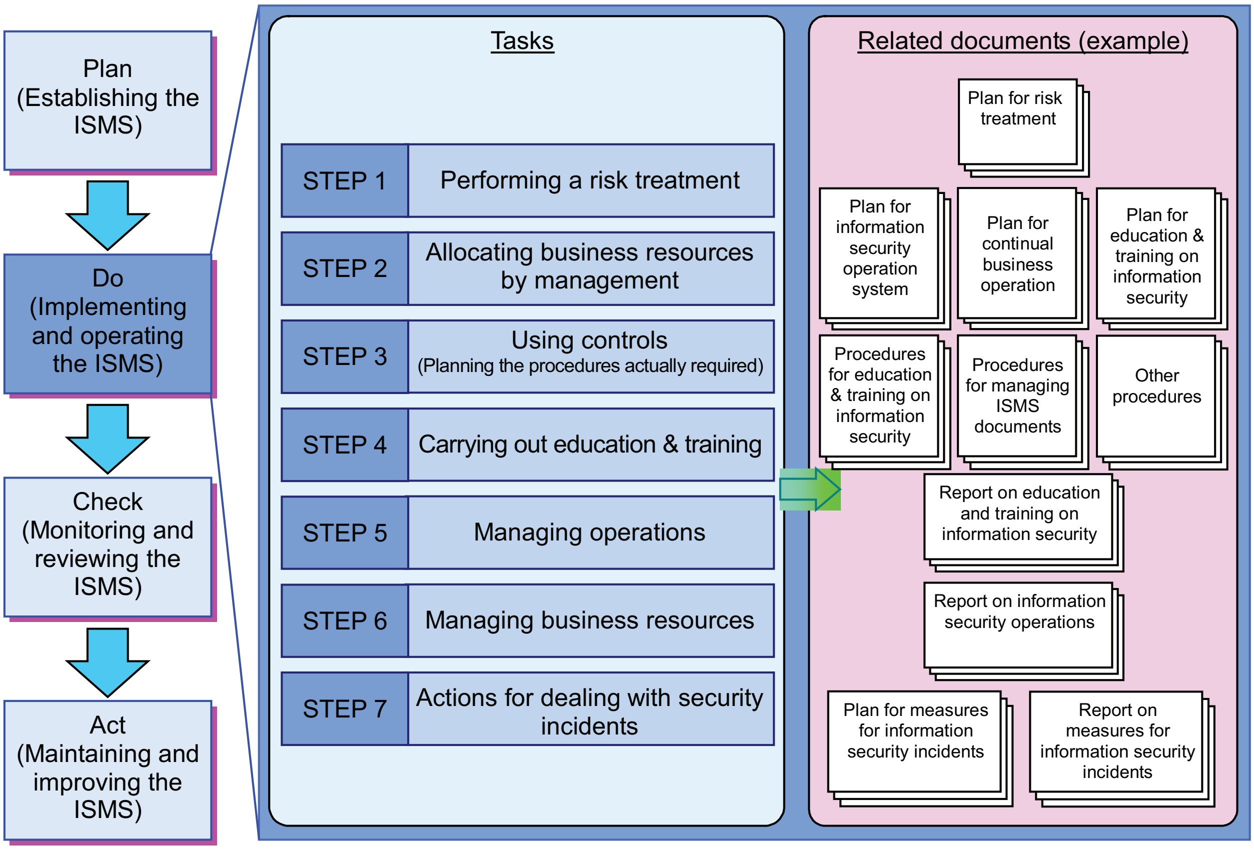

Figure B.5 — Tasks and related documents for implementing and operating the ISMS

B.6 Checking: monitoring and reviewing the ISMS

B.6.1 Need for on-going assurance

The organization, the ISMS and within it the ISMF, will need assurance of its effectiveness both in maintenance of the currently delivered level of security and in its continuous improvement in line with the information security strategy, aligned to the organization's goals.

B.6.2 Compliance assessment

B.6.2.1 Self-assessment

At the most basic level, and especially where the implementation of ISO/IEC 27001 is purely for internal purposes, an assessment by a small team from elsewhere in the organization will give some indication of the effectiveness of the ISMS. However, this approach can often be compromised by peer-group loyalties and personal and organizational obligations.

B.6.2.2 Peer review

A very similar, but alternative, option is to arrange a peer review, where the different organizational loyalties of the peer reviewers give rise to an increase in objectivity and thus assurance.

This option can again be effectively at no cost if the arrangement is made reciprocally, between Information Security Officers. However, this can of course mean that there could be an agreement for mutually positive reports.

B.6.2.3 Independent audit

Independent audits can be obtained from a variety of sources, such as auditing and consultancy firms or an organization's own internal auditors, at only limited cost. The resulting report is likely to be reliable and of higher quality reflecting a typically higher level of expertise. Such audits also bring with them a degree of "benchmarking" in as much as the personnel involved are likely to have performed other such independent audits from which they can draw comparisons.

B.6.2.4 Certification audit against ISO/IEC 27001

Certification audits typically encompass a scoping session, a document review and then the audit of compliance itself.

Based on the experience gained by other certified organizations, healthcare organisations should engage their auditors as soon as they have decided to seek certification. The auditor then becomes more of a partner in the exercise and compliance can be achieved progressively, by initial agreement that the scope statement discussed in B.4.1 is correctly framed and deliverable. However, it is also worth considering a peer review or independent audit at an interim stage to further limit any potential for failure.

A common misconception is that certification is only granted when the observed information security is somehow "perfect". The requisites are merely to have an ISMS that is already operating, a clear understanding of risks and exposures, and a management plan for reducing those exposures to an acceptable level. Indeed, during the auditing process, a limited number of faults can be identified that, subject to their materiality, will not prevent successful certification.

There is also a misperception that certification is time consuming. Yet experience has shown that certification audits of health organizations rarely require more than 5 to 6 days effort by the certification auditor.

The ultimate independent audit is that provided under the guidelines provided by ISO/IEC 27001, as performed by a competent independent auditing body, such as are established in many countries. This audit will be the most thorough of the options listed here, as it will be performed by a competent auditor.

Such an auditor should also be competent in IT and Information Security. Both the rigour of the audit and benchmarking of practice that can be expected from such an audit are therefore high. However, experience has shown that the cost of such an audit is still of an acceptable scale.

Users of this International Standard who choose to follow this route are strongly advised to engage such auditors at the start of their programme such that their support and "buy-in" are obtained progressively and so that their ultimate approval is more likely, given that there will be no 'surprises' at the final audit stage.

B.6.3 Summary

The tasks involved in monitoring and reviewing the ISMS and the related documents produced are summarized in Figure B.6.

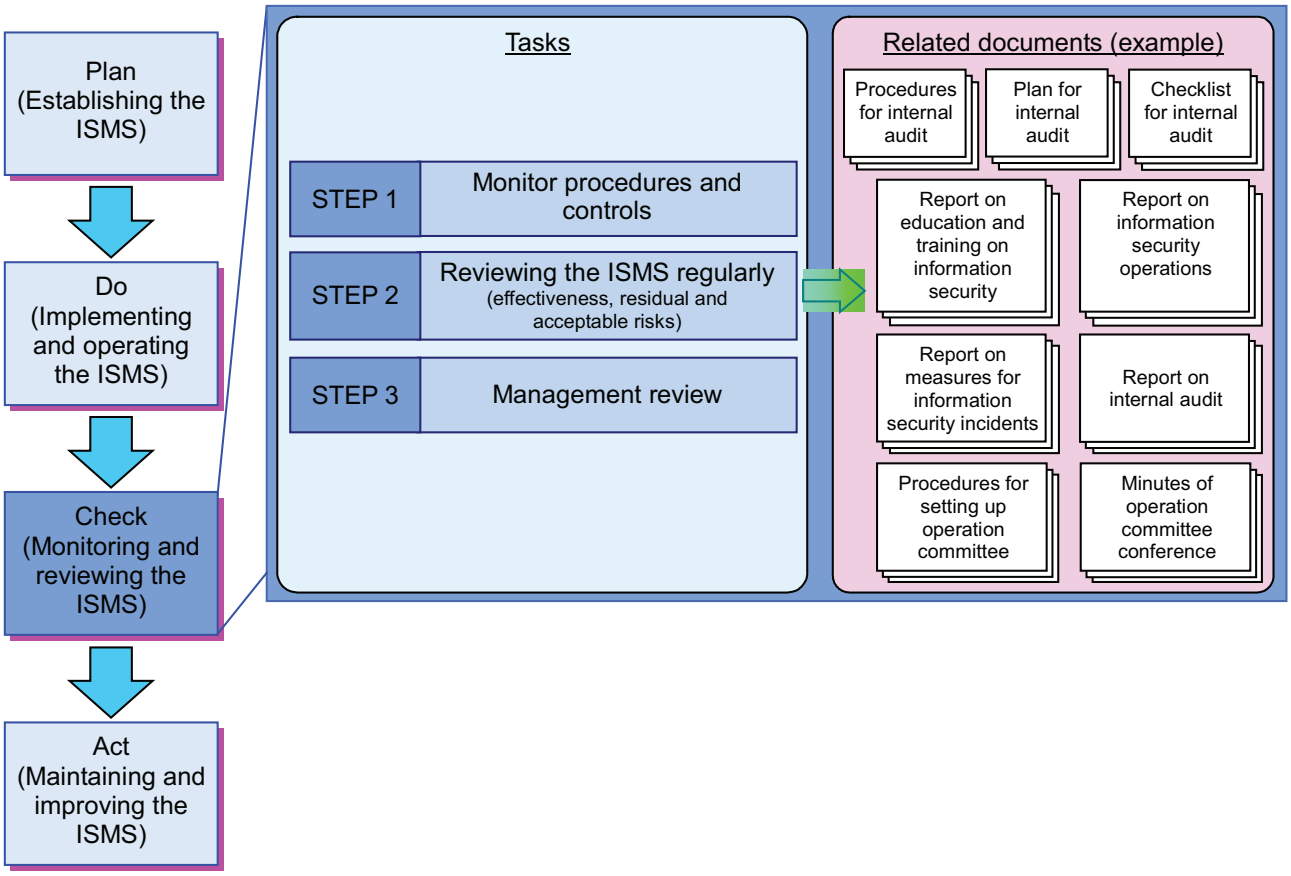

Figure B.6 — Tasks and related documents for monitoring and reviewing the ISMS

B.7 Acting: maintaining and improving the ISMS

Results of the monitoring activities described in the previous clause must return to the ISMF for further consideration as it is the ISMF that is responsible for ensuring that deficiencies are corrected and that the ISMS remains operationally effective.

The statement of applicability described in B.4.7 can be an effective tool for keeping those responsible for clinical and corporate governance appraised of the current state of the ISMS. The format used is also typically suitable for use as an assessment or evidence tool in support of external auditing, clinical assurance and other regulatory inspections.

The security improvement plan described in B.4.6 is also an important tool in demonstrating progress and process improvement.

The tasks and related documents for maintaining and improving the ISMS are summarized in Figure B.7.

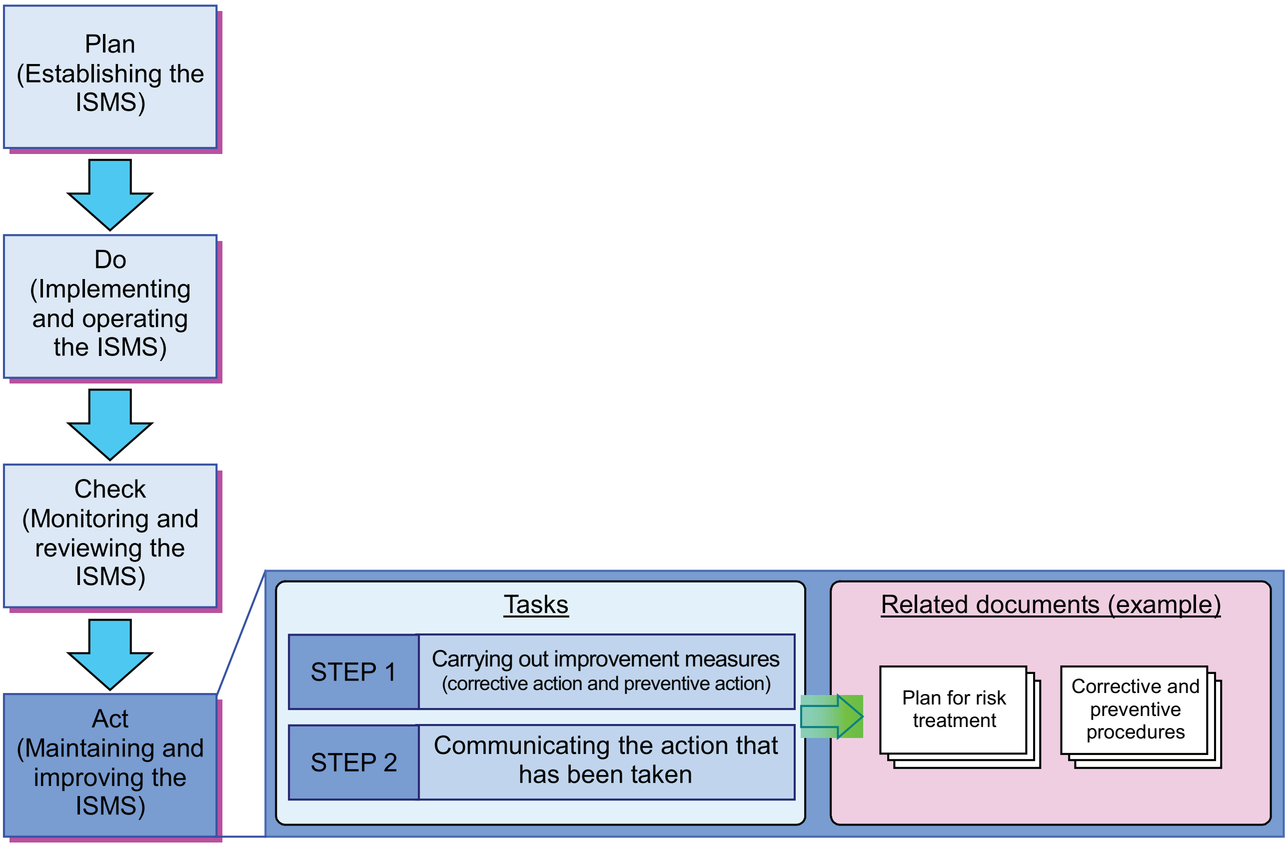

Figure B.7 — Tasks and related documents for monitoring, reviewing, maintaining and improving the ISMS

Annex C
(informative)

Checklist for conformance to ISO 27799

C.1 Instructions for completing the checklist

The checklist in Table C.1 is intended to help organizations processing personal health information determine whether they conform to this International Standard. It lists the controls from this International Standard and contains columns to check where conformance to the controls has been achieved. What follows is an explanation of the columns.

a) Clause: the numbers in the leftmost column corresponds to the clause numbers in the International Standard.

b) Implemented: whether the control is implemented

   1) Yes: the control is implemented and operational.

   2) No: the control is not implemented and operational. The work might be initiated but cannot be said to be fully implemented and in operation within the organization on an ongoing basis.

   Alternatively, the present overall compliance can be presented in percentage figures.

c) Priority: the priority that the organization intends to give the implementation of the control. Recommended to be on a scale of numbers 1, 2, 3, etc., where 1 is the highest priority.

d) Reference document, decision, or diary number: reference to supporting organizational documentation, where applicable.

e) Budgeted: whether implementation of the control has been budgeted (where applicable).

f) Responsible: where the control has not been implemented and operationalized, the name of the person or organizational entity who is nominated by the organization to be responsible for the work of implementing/operationalizing the control.

g) Note: any relevant comments on the control, where applicable.

h) Follow-up: note of what follow-up is planned or performed, where applicable.

The checklist can be used during all types of internal and external auditing and assessment of information security-related work of any organization processing personal health information. The list is designed to give a good overview over the information security situation and also easily be a support for follow-ups.

Table C.1 — Information security controls — Check list for ISO 27799

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
5.1	Management direction for information security								
5.1.1	Policies for information security								
1	Is there a written information security policy?							(Would or should demand?)	
2	Is the written information security policy approved by management?							(Would or should demand?)	

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
3	Is the written information security policy published, and the communicated to all employees and relevant external parties? (how, where, when?)							(Would or should demand?)	
4	Does the information security policy express:								
A	— the need for health information security?								
B	— the goals of health information security?								
C	— compliance scope, as described in 0.0.0.0?								
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 identification of processes and systems that are vital in health care (i.e. failure may lead to adverse patient effects)								
G	— the breadth of health information?								
H	— the rights and ethical responsibilities of staff, as agreed in law, and as accepted by members of professional bodies?								
I	— the rights of subjects of care, where applicable, to privacy and to access to their records?								
J	— the obligations of clinicians with respect to obtaining informational consent from subjects of care and maintaining the confidentiality of personal health information?								
K	— the legitimate needs of clinicians and health organizations to be able to overcome normal security protocols when healthcare priorities, often linked to the incapacity of certain subjects of care to express their preferences, necessitate such overrides; also the procedures to be employed to achieve this?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
L	— the obligations of the respective health organizations, and of subjects of care, where healthcare is delivered on a "shared care" or "extended care" basis?								
M	— the protocols and procedures to be applied to the sharing of information for the purposes of research and clinical trials?								
N	— the arrangements for, and authority limits of, temporary staff, such as locums, students and "on-call" staff?								
O	— the arrangements for, and limitations placed upon, access to personal health information by volunteers and support staff such as clergy and charity personnel?								
P	— the implications of security measures on patient safety?								
Q	q) the implications of information security measures on the performance of health information systems?								
5.1.2	Review of the policies for information security								
1	Is there an ongoing staged review that addresses the totality of the policy annually?								
2	Is the policy reviewed after the occurrence of a serious security incident?								
	In addition to following the guidance given by ISO/IEC 27002, does the review address:								
A	— the changing nature of the health organization's operations and the concomitant changes to risk profile and risk management needs?								
B	— the changes made to the IT infrastructure of the organization, and the concomitant changes these bring to the organization's risk profile?								
C	— the changes identified in the external environment that similarly impact the organization's risk profile?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
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 information privacy commissioners regarding the protection of personal health information?								
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. privacy commissioners)?								
H	— reports on patient safety incidents in order to devise mitigations in those cases where the effectiveness patient safety incident is the result of failures of information security measures								
6.1	Internal organization								
6.1.1	Information security roles and responsibilities								
1	Does the organization:								
A	— clearly define and assign information security responsibilities?								
B	— have an Information Security Management Forum (ISMF) in place to ensure that there is clear direction and visible management support for security initiatives involving the security of health information, as described in 0? Where:								
B1	— is there at a minimum, at least one individual responsible for health information security within the organization?								
B2	— is there a health information security forum that meet regularly, on a monthly or near-to-monthly basis?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
B3	— is there a produced formal scope statement that defines the boundary of compliance activities in terms of people, processes, places, platforms and applications?								
B4	— is there an information security officer that, among other duties, report to the ISMF and provide it with secretariat services?								
B5	— is the officer responsible for collecting, reporting and commenting on the reports received by forum members?								
B6	— is the scope of the statement widely publicized and reviewed within the organization to ensure the adoption of the statement by the organization's information, clinical and corporate governance groups?								
6.1.2	Segregation of duties								
1	In addition to the control given by ISO/IEC 27002, does the organization, where feasible, segregate duties and areas of responsibility in order to reduce opportunities for unauthorized modification or misuse of personal health information?								
6.1.3	Contact with authorities								
	No additional guidance								
6.1.4	Contact with special interest groups								
	No additional guidance								
6.1.5	Information security in project management								
1	Is patient safety considered as a project risk in projects that involves the processing of personal health information?								
6.2	Mobile devices and teleworking								
6.2.1	Mobile device policy								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization also:								
A	— specifically assess the risks involved when using mobile devices in healthcare?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
B	— have a policy on the precautions to be taken when using mobile computing devices, including guidance and restrictions on the use of personal devices within the organisation, together with controls to meet jurisdictional privacy requirements?								
C	— require their mobile users to follow this policy?								
6.2.2	Teleworking								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization also:								
A	— prepare policy on the precautions to be taken when teleworking?								
B	— ensure that teleworking users of health information systems abide by this policy?								
7.1	Prior to employment								
7.1.1	Screening								
1	Does the organization whose staff, contractors or volunteers process (or are expected to process) personal health information verify at the time of job application each applicant's:								
A	— identity?								
B	— current address?								
C	— previous employment?								
D	— applicable health professional qualifications where such are professionally accredited (e.g. physicians, nurses, etc.)?								
2	Does the organization, when an individual is hired for a specific information security role, make sure that the candidate:								
A	— has the necessary competence to perform the security role?								
B	— can be trusted to take the role, especially if the role is critical for the organization?								
7.1.2	Terms and conditions of employment								
1	in addition to the controls given by ISO/IEC 27002, does the organization, whose staff members are involved in processing personal health information, also:								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
A	— document such involvement in relevant job descriptions?								
B	— document relevant job descriptions for security roles and responsibilities as laid down in the organization's information security policy?								
C	— pay special attention to the roles and responsibilities of temporary or short-term staff such as locums, students, interns, etc.?								
2	in addition to following the guidance given by ISO/IEC 27002, does the organization also:								
A	— ensure that employees or contractors have a duty to report breaches of health information security or patient privacy?								
B	— wherever possible, undertake criminal background checks, where not already carried out as part of a health professional accreditation?								
7.2	During employment								
7.2.1	Management responsibilities								
	No specific question (but see guidance in 7.2.1)								
7.2.2	Information security awareness, education and training								
1	In addition to implementing the controls given by ISO/IEC 27002, does the organization also:								
A	— ensure that information security education and training are provided on induction and that regular updates in organizational security policies and procedures are provided to all employees and, where relevant, third-party contractors, researchers, students and volunteers who process personal health information?								
2	— make employees of the organization and where relevant, third-party contractors, aware of disciplinary process and consequences with respect to breaches of information security?								
7.2.3	Disciplinary process								
1	In addition to following the guidance given by ISO/IEC 27002, does the health organization, also:								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
A	— follow procedures that are reflected in policy and thus known to the subject(s) of the disciplinary process?								
B	— in addition to complying with applicable laws, comply with the agreements reached between health professionals and health professional bodies?								
7.3	Termination and change of employment								
7.3.1	Termination or change of employment responsibilities								
1	— is there a process to ensure the termination of previous rights that are no longer required for staff after a change of role in the same way as for individuals who are leaving the organization's employ?								
8.1	Responsibility for assets								
8.1.1	Inventory of assets								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization that process personal health information, also:								
A	— account for health information assets (i.e. maintain an inventory of such assets)?								
B	— have a designated custodian of these health information assets?								
C	— have rules for acceptable use of these assets that are identified, documented and implemented?								
2	Does the organization have rules for maintaining the currency of information assets (e.g. the currency of a drug database) and the integrity of these assets (e.g. the functional integrity of medical devices that record or report data)?								
3	Are medical devices that record or report data uniquely identified?								
4	Does such unique identification of medical devices also take into account that such devices may require special security considerations in relation to the environment in which they operate?								
5	Does such unique identification of medical devices also take into account the electromagnetic emissions that occur during their operation?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
8.1.2	Ownership of assets								
	No additional guidance								
8.1.3	Acceptable use of assets								
	No additional guidance								
8.1.4	Return of assets								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization ensure that all employees and contractors, upon termination of employment, return all personal health information in their possession that is in non-electronic form and ensure that all personal health information in their possession in electronic form is updated on relevant systems and then securely deleted from any devices on which it has resided?								
8.2	Information classification								
8.2.1	Classification of information								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization uniformly classify personal health information confidential?								
2	Is personal health information subject to suitably careful protection at all times?								
3	Is criticality identified through a risk assessment with respect to:								
A	— traditional classification of data on the basis of its sensitivity to disclosure?								
B	— the extent to which the availability and integrity of the information are essential for the ongoing provision of healthcare?								
C	— processes, IT devices, software, locations and personnel?								
8.2.2	Labelling of information								
1	Do all health information systems processing personal health information inform users of the confidentiality of personal health information accessible from the system (e.g. at start-up or log-in)?								
2	Is hardcopy output labelled as confidential when it contains personal health information?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
3	Are users of the health information systems able to recognize when they access personal health information?								
8.2.3	Handling of assets								
	No additional guidance								
8.3	Media handling								
8.3.1	Management of removable media								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization ensure that:								
A	— media containing personal health information is either physically protected or else encrypted?								
B	— status and location of media containing unencrypted personal health information is monitored?								
C	— media containing personal health information is encrypted while its media are in transit?								
D	— media containing personal health information is protected from theft while its media are in transit?								
8.3.2	Disposal of media								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization ensure that:								
A	— all personal health information securely is erased or else the media destroyed when no longer required for use?								
A1	— secure disposal of data is performed prior to repair or disposal?								
A2	— secure disposal of data is also performed on medical devices that record or report data?								
8.3.3	Physical media transfer								
	No additional guidance								
9.1	Business requirements of access control								
9.1.1	Access control policy								
1	Does the organization control access to personal health information?								
2	Do the users of health information systems generally only access personal health information:								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
A	— when a healthcare relationship exists between the user and 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?								
3	Does the organization have an access control policy governing access to personal health information?								
4	Is the organization's policy on access control established on the basis of predefined roles with associated authorities which are consistent with, but limited to, the needs of that role?								
5	Does the access control policy, as a component of the information security policy framework described in 5.1.1:								
A	— reflect professional, ethical, legal and subject-of-care-related requirements?								
B	— take into account the tasks performed by health professionals and the task's workflow?								
6	Does the organization identify and document all parties with whom patient data is exchanged?								
A	Are contractual agreements made with these parties regulating access and privileges, prior to exchange of patient data?								
7	Are the authorizations in policies and processes clear enough to meet requirement to override "normal" access controls in emergency situations?								
8	Are federated identity and access management solutions implemented?								
9.1.2	Access to networks and network services								
9.2	User access management								
9.2.1	User registration and de-registration								
1	Is there a formal user registration process for users that access systems that process personal health information?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
2	Do the user registration procedures ensure that the level of authentication required of claimed user identity is consistent with the level(s) of access that will become available to the user?								
3	Are user registration details periodically re-viewed to ensure that they are complete, accurate and that access is still required?								
4	In addition to the guidance given by ISO/IEC 27002, does the task of identify-ing and registering users of health information systems include all of the following:								
A	— the accurate capture of a user's identity (e.g. Joan Smith, born March 26th 1982, currently resident at a specific address);								
B	— the accurate capture, after verification, of a user's enduring profes-sional credentials (e.g. Dr. Joan Smith, cardiol-ogist) and/or job title (e.g. Susan Jones, Medical Receptionist)?								
C	— the assignment of an un-ambiguous user identifier?								
9.2.2	User access provisioning								
1	Does the user access provisioning procedures clearly determine whether user6s will or will not have access to personal health information?								
9.2.3	Management of privileged access rights								
1	In addition to following the guidance given by ISO/ IEC 27002, do the health information systems con-taining personal health information support role-based access control capable of mapping each user to one or more roles, and each role to one or more system functions?								
2	Does a user of a health information system con-taining personal health information access its services in a single role?								
3	Do users who have been registered with more than one role designate a single role during each health information system access session?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
4	Do health information systems associate users (including health professionals, supporting staff and others) with the records of subjects of care and allow future access based on this association?								
9.2.4	Management of secret authentication information of users								
	No additional guidance								
9.2.5	Review of user access rights								
1	In addition to the guidance given by ISO/IEC 27002, is special consideration given to users who will reasonably be expected to provide emergency care where they may need access to personal health information in emergency situations where a subject of care may be unable to communicate consent?								
9.2.6	Removal or adjustment of access rights								
1	Does the organization terminate as soon as possible the user access privileges with respect to such information for any departing permanent or temporary employee, third-party contractor or volunteer upon termination of employment, contracting or volunteer activities?								
2	In addition to the guidance given by ISO/IEC 27002, does the timely termination of short-time access privileges after internship, locum, etc. take into account that many transactions take place well after the time of care (e.g. the sign-off of medical transcriptions)?								
3	Does the organization seriously consider immediate termination of access rights following the supply of a resignation notice, notice of dismissal, etc. wherever an increased risk is perceived from the continuation of such access?								
9.3	User responsibilities								
9.3.1	Use of secret authentication information								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
1	In addition to following the guidance given by ISO/IEC 27002, does the organization, when determining user responsibilities, respect the rights and ethical responsibilities of health professionals, as agreed in law and as accepted by members of health professional bodies?								
9.4	System and application access control								
9.4.1	Information access restriction								
1	Do health information systems processing personal health information authenticate users by means of authentication involving at least two factors?								
2	In addition to the guidance given by ISO/IEC 27002, is special consideration given to the technical measures by which a subject of care is securely authenticated when accessing all or part of his/her own information (in those health information systems that permit such access)?								
3	Is similar emphasis also given to the ease of use of such measures, especially for handicapped subjects of care, and to provisions for access by substitute decision makers?								
9.4.2	Secure log-on procedures								
	No additional guidance								
9.4.3	Password management system								
	No additional guidance								
9.4.4	Use of privileged utility programs								
	No additional guidance								
9.4.5	Access control to program source code								
	No additional guidance								
10.1	Cryptographic controls								
10.1.1	Policy on the use of cryptographic controls								
	No additional guidance								
10.1.2	Key management								
	No additional guidance								
11.1	Secure areas								
11.1.1	Physical security perimeter								
1	Does the organization use security perimeters to protect areas that contain health information processing facilities?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
2	Are these secure areas protected by appropriate entry controls to ensure that only authorized personnel are allowed access?								
3	Are physical security measures for information coordinated with physical security and safety measures for subjects of care?								
4	Do the physical security measures for information coordinated with physical security and safety measures take into account that clients in healthcare are often unable to physically provide for their own personal safety and security?								
11.1.2	Physical entry controls								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization take sensible steps to ensure that the public are only as close to IT equipment (servers, storage devices, terminals and displays) as physical constraints and clinical processes demand?								
11.1.3	Securing offices, rooms and facilities								
	No additional guidance								
11.1.4	Protecting against external and environmental threats								
1	As above for 11.1.2 applies								
11.1.5	Working in secure areas								
	No additional guidance								
11.1.6	Delivery and loading areas								
1	Are the physical areas in healthcare that gather health information through interview and that contain systems where data are viewed on screen subject to additional scrutiny considering the distinct circumstances following the provision of healthcare to the public?								
2	Does the organization consider providing reminders to curtail discussion of patient cases in public areas?								
11.2	Equipment								
11.2.1	Equipment siting and protection								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
1	In addition to following the guidance given by ISO/IEC 27002, does the organization situate any workstations allowing access to personal health information in a way that prevents unintended viewing or access by subjects of care and the public?								
2	Does the organization ensure that the siting and protection guidelines for IT equipment, in relation to the environment, minimize exposure to such emissions that may occur during their operation? [This is especially applicable to hospital organizations.]								
11.2.2	Supporting utilities								
	No additional guidance								
11.2.3	Cabling security								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization give serious consideration to the shielding of network and other cabling in areas with high emissions from medical devices?								
11.2.4	In addition to following the guidance given by ISO/IEC 27002, does the organization give serious consideration to the shielding of equipment in areas with high emissions from medical devices?								
11.2.5	In addition to implementing the control given by ISO/IEC 27002, does the organization, when providing or using equipment, data or software to support a healthcare application containing personal health information, not allow such equipment, data or software to be removed from the site or relocated within it without authorization by the organization?								
11.2.6	Security of equipment and assets off-premises								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization ensure that any use, outside its premises, of medical devices that record or report data has been authorized?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
2	Do the devices referred to in item 1 above include equipment used by remote workers, even where such usage is perpetual (i.e. where it forms a core feature of the employee's role, such as for ambulance personnel, therapists, etc.)?								
11.2.7	Secure disposal or re-use of equipment								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization securely erase or else destroy all media containing health information application software or personal health information when the media are no longer required for use?								
11.2.8	Unattended user equipment								
1	No additional guidance for information security management in health (but see also 9.3, User responsibilities)								
11.2.9	Clear desk and clear screen policy								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization, when determining user responsibilities, respect the rights and ethical responsibilities of health professionals, as agreed in law and as accepted by members of health professional bodies?								
12.1	Operational procedures and responsibilities								
12.1.1	Documented operating procedures								
	No additional guidance								
12.1.2	Change management								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization control changes to information processing facilities and systems that process personal health information by means of a formal and structured change control process to ensure the appropriate control of host applications and systems and continuity of patient care?								
2	Does the change process, due to the potentially disastrous consequences for patient care and safety of inappropriate, inadequately tested or incorrect changes, explicitly record and assess the risks of the change?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
12.1.3	Capacity management								
	No additional guidance								
12.1.4	Separation of development, testing and operational environments								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization separate (physically or virtually) development and testing environments for health information systems processing such information from operational environments hosting those health information systems?								
2	Are rules defined and documented for the migration of software from development to operational status by the organization hosting the affected application(s)?								
12.2	Protection from malware								
12.2.1	Controls against malware								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization implement appropriate prevention, detection and response controls to protect against malicious software?								
2	Does the organization implement appropriate user awareness training to protect against malicious software?								
12.3	Backup								
12.3.1	Information backup								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization back up all personal health information and store it in a physically secure environment to ensure its future availability?								
2	Does the organization, in order to protect confidentiality, back up personal health information in an encrypted format?								
12.4	Logging and monitoring								
12.4.1	Event logging								
1	Do the health information systems processing personal health information, create a secure audit record each time a user accesses, creates, updates or archives personal health information via the system?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
2	Does the audit log uniquely identify the user, uniquely identify the data subject (i.e. the subject of care), identify the function performed by the user (record creation, access, update, etc.), and note the time and date at which the function was performed?								
3	When personal health information is updated, is a record of the former content of the data and the associated audit record (i.e. who entered the data on what date) retained?								
4	When messaging systems are used to transmit messages containing personal health information:								
A	Is there a log of such message transmissions?								
B	Does that log contain the time, date, origin and destination of the message, but not its content?								
5	Is there a carefully assessed and determined retention period for these audit logs, with particular reference to clinical professional standards and legal obligations, in order to enable investigations to be carried out when necessary and to provide evidence of misuse where necessary?								
6	Is the health information system's audit logging facility operational at all times while the health information system being audited is available for use?								
7	Are health information systems containing personal health information provided with facilities for analysing logs and audit trails that:								
A	Allow the identification of all system users who have accessed or modified a given subject of care's record(s) over a given period of time?								
B	Allow the identification of all subjects of care whose records have been accessed or modified by a given system user over a given period of time?								
12.4.2	Protection of log information								
1	Are audit records secure and tamper-proof?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
2	Is access to system audit tools and audit trails safeguarded to prevent misuse or compromise?								
	[There are many Health-specific implementation guidances in relation to protection of log information that are not included in this document], applies								
12.4.3	Administrator and operator logs								
	No additional guidance								
12.4.4	Clock synchronisation								
1	Do health information systems supporting time-critical-shared care activities provide time synchronization services to support tracing and reconstitution of activity timelines where required?								
12.5	Control of operational software								
12.5.1	Installation of software on operational systems								
	No additional guidance								
12.6	Technical vulnerability management								
12.6.1	Management of technical vulnerabilities								
	No additional guidance								
12.6.2	Restrictions on software installation								
1	Are rules governing the installation of software by users established and implemented?								
12.7	Information systems audit considerations								
12.7.1	Information systems audit controls								
	No additional guidance								
13.1	Network security management								
13.1.1	Network controls								
	No additional guidance								
13.1.2	Security of network services								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization carefully consider what impact the loss of network service availability will have upon clinical practice?								
13.1.3	Segregation in networks								
	No additional guidance								
13.2	Information transfer								
13.2.1	Information transfer policies and procedures								
1	Does the organization ensure that the security of such information exchange is the subject of policy development and compliance audit?								
13.2.2	Agreements on information transfer								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
	No additional guidance								
13.2.3	Electronic messaging								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization, when transmitting personal health information by electronic messaging, ensure its confidentiality and integrity?								
2	Are e-mail between health professionals that contain personal health information encrypted in transit?								
13.2.4	Confidentiality or non-disclosure agreements								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization have a confidentiality agreement in place that specifies the confidential nature of this information?								
2	Is the agreement applicable to all personnel accessing health information?								
3	Does the agreement above include reference to the penalties that are possible when a breach in the information security policy is identified?								
14.1	Security requirements of information systems								
14.1.1	Information security requirements analysis and specification								
14.1.1.1	Uniquely identifying subjects of care								
1	Do the health information systems processing personal health information ensure that each subject of care can be uniquely identified within the system?								
2	Are health information systems processing personal health information capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency?								
3	Does the organization ensure that data from which personal identification can be derived is 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?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
14.1.1.2	Output data validation								
1	Do health information systems processing personal health information provide personally identifying information to assist health professionals in confirming that the electronic health record retrieved matches the subject of care under treatment?								
2	Do health information systems make it possible to check that hardcopy printouts are complete?								
14.1.2	Securing application services on public networks								
	No additional guidance								
14.1.3	Protecting application services transactions								
	(See Health-specific implementation guidance in 14.1.2)								
14.1.3.1	Publicly available health information								
1	Is publicly available health information (as distinct from personal health information) archived?								
2	Is the integrity of publicly available health information protected to prevent unauthorized modification?								
3	Is the source (authorship) of publicly available health information stated and its integrity protected?								
14.2	Security in development and support processes								
14.2.1	Secure development policy								
	No additional guidance								
14.2.2	System change control procedures								
	No additional guidance								
14.2.3	Technical review of applications after operating platform changes								
	No additional guidance								
14.2.4	Restrictions on changes to software packages								
	No additional guidance								
14.2.5	Secure system engineering principles								
	No additional guidance								
14.2.6	Secure development environment								
	No additional guidance								
14.2.7	Outsourced development								
	No additional guidance								
14.2.8	System security testing								
	No additional guidance								
14.2.9	System acceptance testing								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
1	In addition to implementing the control given by ISO/IEC 27002, does the organization have established acceptance criteria for planned new information systems, upgrades and new versions?								
2	Are such suitable tests of the system carried out prior to acceptance?								
3	Are clinical users involved in the testing of clinically relevant system features?								
14.3	Test data								
14.3.1	Protection of test data								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization ensure that no actual personal health information is used as test data?								
15.1	Information security in supplier relationships								
15.1.1	Information security policy for supplier relationships								
1	In addition to implementing the control given by ISO/IEC 27002, does the organization assess the risks associated with access by external parties to these systems or the data they contain, and then implement security controls that are appropriate to the identified level of risk and to the technologies employed?								
15.1.2	Addressing security within supplier agreements								
	No additional guidance								
15.1.3	Information and communication technology supply chain								
	No additional guidance								
15.2	Supplier service delivery management								
15.2.1	Monitoring and review of supplier services								
	No additional guidance								
15.2.2	Managing changes to supplier services								
	No additional guidance								
16.1	Management of information security incidents and improvements								
16.1.1	Responsibilities and procedures								
	No additional guidance								
16.1.2	Reporting information security events								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization have security incident management responsibilities and procedures that:								
A	— ensure effective and timely response to security incidents?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
B	— ensure that there is an effective and prioritized escalation path for incidents such that crisis management and business continuity management plans can be invoked in the right circumstances and at the right time?								
C	— collect and preserve incident-related audit logs and other relevant evidence?								
2	Does the organization inform the subject of care whenever personal health information has been unintentionally disclosed?								
3	Does the organization inform the subject of care whenever lack of availability of health information systems may have adversely affected their care?								
4	Does the organization perform an information security assessment on incidents that could led to, disguise misuse of or erroneous use of IT equipment or events that could otherwise imply an information security incident such as fire, brake-in or theft of hardware?								
16.1.3	Reporting information security weaknesses								
	No additional guidance								
16.1.4	Assessment of and decision on information security events								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization processing personal health information assess whether the information security event involved personal health information?								
16.1.5	Response to information security incidents								
	No additional guidance								
16.1.6	Learning from information security incidents								
	No additional guidance								
16.1.7	Collection of evidence								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization consider the implications of collecting evidence for purposes of establishing medical malpractice, and also to consider inter-jurisdictional requirements when health information systems are accessible across jurisdictional boundaries?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
17.1	Information security continuity								
17.1.1	Planning information security continuity								
1	Does the organization ensure that business continuity management includes health crisis management planning?								
2	Is the organization cognizant of the role that health information systems play in patient continuity of care?								
3	Is the organization prepared if/when IT systems fail?								
17.1.2	Implementing information security continuity								
1	In addition to the guidance given by ISO/IEC 27002, does the organization identify processes, systems and other relevant equipment that are vital in health care delivery?								
2	Are fall-back procedures considered as necessary in order to counter failure in processes, systems and relevant equipment that are vital in health care delivery?								
17.1.3	Verify, review and evaluate information security continuity								
	No additional guidance								
17.2	Redundancies								
17.2.1	Availability of information processing facilities								
	No additional guidance								
18.1	Compliance with legal and contractual requirements								
18.1.1	Identification of applicable legislation and contractual requirements								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization put a compliance auditing programme in place that addresses the full life cycle of operations, not just of those processes that identify issues, but also of those that review outcomes and that decide on updates to the ISMS?								
2	Are the organization's audit programmes formally structured to cover all elements of this International Standard, all areas of risk and all implemented controls, within a 12 month to 18 month cycle?								

Table C.1 *(continued)*

Clause	Control	Yes	No	Priority	Reference document	Budgeted	Responsible	Note	Follow-up
3	Does the ISMF set itself the objective of establishing a graduated compliance auditing framework, whose bottom layer is self-audit by the process operators and managers?								
4	Are, thereafter, the auditing of the ISMS, on behalf of the ISMF, internal auditing, controls assurance assessments and external audits, defined in a manner that allows each layer to draw confidence from all of the layers below it?								
18.1.2	Intellectual property rights								
	No additional guidance								
18.1.3	Protection of records								
	No additional guidance								
18.1.4	Privacy and protection of personally identifiable information								
1	In addition to following the guidance given by ISO/IEC 27002, does the organization manage informational consent of subjects of care?								
2	Where possible, is informational consent of subjects of care obtained before personal health information is e-mailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organization?								
18.1.5	Regulation of cryptographic controls								
	No additional guidance								
18.2	Information security reviews								
18.2.1	Independent review of information security								
	No additional guidance								
18.2.2	Compliance with security policies and standards								
	No additional guidance								
18.2.3	Technical compliance review								
	No additional guidance								

Bibliography

[1] ISO/IEC 11770-1, *Information technology — Security techniques — Key management — Part 1: Framework*

[2] ISO/IEC 11770-2, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*

[3] ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

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

[5] ISO 15489-1, *Information and documentation — Records management — Part 1: General*

[6] ISO 17090-1, *Health informatics — Public key infrastructure — Part 1: Overview of digital certificate services*

[7] ISO 17090-2, *Health informatics — Public key infrastructure — Part 2: Certificate profile*

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

[9] ISO/TR 17791:2013, *Health informatics — Guidance on standards for enabling safety in health software*

[10] ISO/TS 17975, *Health informatics — Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information*

[11] ISO/IEC 18028-4:2005, *Information technology -- Security techniques -- IT network security -- Part 4: Securing remote access*[5)]

[12] ISO 21091, *Health informatics – Directory services for healthcare providers, subjects of care and other entities*

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

[14] ISO 22301, *Societal security — Business continuity management systems --- Requirements*

[15] ISO 22313, *Societal security — Business continuity management systems — Guidance*

[16] ISO 22600-1, *Health informatics — Privilege management and access control — Part 1: Overview and policy management*

[17] ISO 22600-2, *Health informatics — Privilege management and access control — Part 2: Formal models*

[18] ISO 22600-3, *Health informatics — Privilege management and access control — Part 3: Implementations*

[19] ISO/TS 25237, *Health informatics — Pseudonymization*

[20] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[21] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

5) Withdrawn.

[22] ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[23] ISO/IEC/TR 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*

[24] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[25] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[26] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[27] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[28] ISO/IEC 27033-4, *Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*

[29] ISO/IEC 27033-5, *Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*

[30] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*

[31] ISO/IEC 27036-1, *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*

[32] ISO/IEC 27036-2, *Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements*

[33] ISO/IEC 27036-3, *Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security*

[34] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[35] ISO 27789:2013, *Health informatics — Audit trails for electronic health records*

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

[37] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[38] ISO/IEC 29101, *Information technology — Security techniques — Privacy architecture framework*

[39] ISO 31000, *Risk management — Principles and guidelines*

ICS 35.240.80
Price based on 99 pages

AENOR Asociación Española de Normalización y Certificación

Génova, 6
28004 MADRID-Spain

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032