BRITISH STANDARD

BS EN ISO 27799:2008

Health informatics — Information security management in health using ISO/IEC 27002 (ISO 27799:2008)

ICS 35.240.80

BSI British Standards

National foreword

This British Standard is the UK implementation of EN ISO 27799:2008.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2008

ISBN 978 0 580 56326 3

Amendments/corrigenda issued since publication

Date	Comments

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 27799

July 2008

ICS 35.240.80

English Version

Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2008)

Informatique de santé - Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002 (ISO 27799:2008)

Medizinische Informatik - Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 (ISO 27799:2008)

This European Standard was approved by CEN on 15 June 2008.

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 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 Management Centre has the same status as the official versions.

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

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

Management Centre: rue de Stassart, 36 B-1050 Brussels

Ref. No. EN ISO 27799:2008: E

Foreword

This document (EN ISO 27799:2008) 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 January 2009, and conflicting national standards shall be withdrawn at the latest by January 2009.

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.

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, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

Endorsement notice

The text of ISO 27799:2008 has been approved by CEN as a EN ISO 27799:2008 without any modification.

Contents

Page

Foreword ... iv

Introduction ... v

1 Scope ... 1
1.1 General ... 1
1.2 Scope exclusions ... 1

2 Normative references ... 2

3 Terms and definitions ... 2
3.1 Health terms ... 2
3.2 Information security terms ... 3

4 Abbreviated terms ... 5

5 Health information security ... 5
5.1 Health information security goals ... 5
5.2 Information security within information governance ... 6
5.3 Information governance within corporate and clinical governance ... 7
5.4 Health information to be protected ... 7
5.5 Threats and vulnerabilities in health information security ... 8

6 Practical action plan for implementing ISO/IEC 27002 ... 8
6.1 Taxonomy of the ISO/IEC 27002 and ISO/IEC 27001 standards ... 8
6.2 Management commitment to implementing ISO/IEC 27002 ... 9
6.3 Establishing, operating, maintaining and improving the ISMS ... 10
6.4 Planning: establishing the ISMS ... 10
6.5 Doing: implementing and operating the ISMS ... 18
6.6 Checking: monitoring and reviewing the ISMS ... 19
6.7 Acting: maintaining and improving the ISMS ... 20

7 Healthcare implications of ISO/IEC 27002 ... 20
7.1 General ... 20
7.2 Information security policy ... 21
7.3 Organizing information security ... 22
7.4 Asset management ... 25
7.5 Human resources security ... 26
7.6 Physical and environmental security ... 29
7.7 Communications and operations management ... 30
7.8 Access control ... 36
7.9 Information systems acquisition, development and maintenance ... 39
7.10 Information security incident management ... 41
7.11 Information security aspects of business continuity management ... 42
7.12 Compliance ... 42

Annex A (informative) **Threats to health information security** ... 45

Annex B (informative) **Tasks and related documents of the Information Security Management System** ... 50

Annex C (informative) **Potential benefits and required attributes of support tools** ... 54

Bibliography ... 57

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 27799 was prepared by Technical Committee ISO/TC 215, *Health informatics*.

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 by implementing ISO/IEC 27002[1)]. Specifically, this International Standard 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 must 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 must 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.

The need for effective IT security management in healthcare is made all the more urgent by the increasing use of wireless and Internet technologies in healthcare delivery. If not implemented properly, these complex technologies will increase the risks to the confidentiality, integrity and availability of health information. 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 must therefore have clear, concise and healthcare-specific guidance on the selection and implementation of such controls. This guidance must 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, 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 and the United Kingdom. Interest is growing in other countries as well. This International Standard (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 ISO/IEC 27002 or ISO/IEC 27001. Rather, it is a complement to these more generic standards.

This International Standard 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. This International Standard therefore places constraints upon the application of certain security controls specified in ISO/IEC 27002. This in turn has led to the inclusion in Clause 7 of several normative statements stating that the application of a given security control is mandatory. For example, 7.2.1 states that

> *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.*

1) This guideline is consistent with the revised version of ISO/IEC 27002:2005.

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, this International Standard. It is to be hoped, however, that as healthcare organizations strive to improve the security of personal health information, conformance with this International Standard, as a stricter standard for healthcare, will also become widespread.

All of the security control objectives described in ISO/IEC 27002 are relevant to health informatics but some controls require additional explanations with regard to how they can be used best 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.

This International Standard's 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.

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.

Benefits of using this International Standard

ISO/IEC 27002 is a broad and complex standard and its advice is not tailored specifically to healthcare. This International Standard 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 are maintained, that critical health information systems remain available, and that accountability for health information is upheld.

The adoption of this guidance 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 guidance, 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 sections of that International Standard before continuing. Implementers of this Intenational Standard (ISO/IEC 27799) must first thoroughly read ISO/IEC 27002, as the text below will frequently refer the reader to the relevant sections of that International Standard. The present document cannot be fully understood without access to the full text of ISO/IEC 27002.

General readers not already familiar with health information security and its goals, challenges, and broader context, will benefit from reading a brief introduction, to be found in Clause 5.

Readers seeking guidance on how to implement ISO/IEC 27002 in a health environment will find a practical action plan described in Clause 6. No mandatory requirements are contained in this clause. Instead, general advice and guidance are given on how best to proceed with the implementation of 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 eleven security control clauses and 39 main security control categories described in ISO/IEC 27002 will find it in Clause 7. This clause leads the reader through each of the eleven security control clauses of 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.

This International Standard concludes with three informative annexes. Annex A describes the general threats to health information. Annex B briefly describes tasks and related documents of the information security management system. Annex C discusses the advantages of support tools as an aid to implementation. The Bibliography lists related standards in health information security.

INTERNATIONAL STANDARD **ISO 27799:2008(E)**

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

1 Scope

1.1 General

This International Standard defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that standard[2)].

This International Standard specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. 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.

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 electronic storage) and whatever means are used to transmit it (by hand, via fax, over computer networks or by post), as the information must 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, 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 for an understanding of this International Standard.

1.2 Scope exclusions

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 bibliographic Reference [10] for an example of an ISO Technical Specification that deals specifically with this subject);

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

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

2) This guideline is consistent with the revised version of ISO/IEC 27002:2005.

2 Normative references

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

ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1 Health terms

3.1.1
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

[ISO/TR 18307:2001, definition 3.73]

3.1.2
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 authorized users

NOTE Adapted from ISO/TR 20514:2005, definition 2.25.

3.1.3
healthcare
any type of service provided by professionals or paraprofessionals with an impact on health status

[European Parliament, 1998, as cited by WHO]

3.1.4
healthcare organization
generic term used to describe many types of organizations that provide healthcare services

[ISO/TR 18307:2001, definition 3.74]

3.1.5
health professional
person who is authorized by a recognised body to be qualified to perform certain health duties

NOTE Adapted from ISO/TS 17090-1:2002, definition 3.18.

3.1.6
healthcare provider
any person or organization who is involved in, or associated with, the delivery of healthcare to a client, or caring for client wellbeing

3.1.7
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

[ISO 22857:2004, definition 3.7]

3.1.8
patient
subject of care

(See below, **3.1.10**).

3.1.9
personal health information
information about an identifiable person which relates to the physical or mental health of the individual, or to provision of health services to the individual, and which may include:

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

b) information about payments or eligibility for healthcare with 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 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 Personal health information does not include information that, either by itself or when combined with other information available to the holder, is anonymized, i.e. the identity of the individual who is the subject of the information cannot be ascertained from the information.

3.1.10
subject of care
one or more persons scheduled to receive, receiving, or having received a health service

[ISO/TS 18308:2004, definition 3.40]

3.2 Information security terms

3.2.1
asset
anything that has value to the organization

[ISO/IEC 13335-1:2004, definition 2.2]

NOTE In the context of health information security, assets include:

a) health information;

b) IT services;

c) hardware;

d) software;

e) communications facilities;

f) media;

g) IT facilities;

h) medical devices that record or report data.

3.2.2
accountability
property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2:1989, definition 3.3.3]

3.2.3
assurance
result of a set of compliance processes through which an organization achieves confidence in the status of its information security management

3.2.4
availability
property of being accessible and usable upon demand by an authorized entity

[ISO 7498-2:1989, definition 3.3.11]

3.2.5
compliance assessment
processes by which an organization confirms that the information security controls put in place remain both operational and effective

NOTE Legal compliance relates specifically to the security controls put in place to deliver the requirements of relevant legislation such as the European Union Directive on the Protection of Personal Data.

3.2.6
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO 7498-2:1989, definition 3.3.16]

3.2.7
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[ISO 7498-2:1989, definition 3.3.21]

3.2.8
information governance
processes by which an organization obtains assurance that the risks to its information, and thereby the operational capabilities and integrity of the organization, are effectively identified and managed

3.2.9
information security
preservation of confidentiality, integrity and availability of information

NOTE Other properties, particularly accountability of users but also authenticity, non-repudiation, and reliability, are often mentioned as aspects of information security but could be considered as derived from the three core properties in the definition.

3.2.10
risk
combination of the probability of an event and its consequence

[ISO Guide 73:2002, definition 3.1.1]

3.2.11
risk assessment
overall process of risk analysis and risk evaluation

[ISO Guide 73:2002, definition 3.3.1]

3.2.12
risk management
coordinated activities to direct and control an organization with regard to risk

NOTE Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.

[ISO Guide 73:2002, definition 3.1.7]

3.2.13
risk treatment
process of selection and implementation of measures to modify (typically reduce) risk

NOTE Adapted from ISO Guide 73:2002, definition 3.4.1.

3.2.14
system integrity
property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation of the system

3.2.15
threat
potential cause of an unwanted incident, that may result in harm to a system or organization

[ISO/IEC 13335-1:2004, definition 2.25]

3.2.16
vulnerability
weakness of an asset or group of assets that can be exploited by one or more threats

[ISO/IEC 13335-1:2004, definition 2.26]

4 Abbreviated terms

ISMF Information Security Management Forum

ISMS Information Security Management System

IT Information Technology

SLA Service Level Agreement

SOA Statement of Applicability

5 Health information security

5.1 Health information security goals

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 must 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 Clause 7 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. They include:

a) honouring legislative obligations as expressed in applicable data protection laws and regulations protecting a subject of care's right to privacy[3)];

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).

5.2 Information security within information governance[4)]

In recent years, corporate governance has become a critical issue for organizations of all types, in response to the regulatory drives embodied in initiatives such as the United States' Sarbanes Oxley Act and Health Insurance Portability and Accountability Act, the European Basel II Accords, the UK's Turnbull Code and Germany's KontraG. Also, the increasing dependence of organizations on information and its supporting technologies makes information governance an important component of operational risk management processes.

Many areas of information management, such as accreditation and data protection, can be considered to fall within the scope of information governance. It is vitally important that the scope of information governance embrace and aid the ongoing deployment of information security so that due attention is always paid to confidentiality, integrity and availability. Information security is clearly a critical component enabling the broader aspects of information governance.

---

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

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

5.3 Information governance within corporate 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 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 becomes increasingly evident that 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 therefore need to treat effective information security risk management as equal in importance to care treatment plans, infection management strategies and other "core" clinical management matters.

5.4 Health information to be protected

There are several types of information whose confidentiality, integrity and availability[5)] need to be protected:

a) personal health information;

b) pseudonymized data derived from personal health information via 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 with regard to personal health information;

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 [c) above] may not be confidential, but protecting its integrity may be very important. Likewise, audit trail data [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 6.4.4). The results of regular risk assessment must be fitted to the priorities and resources of the implementing organization.

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

5.5 Threats and vulnerabilities in health information security

Types of information security threats and vulnerabilities vary widely, as do their descriptions. While none is 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.

Many health organizations are chronically underfunded and their staff members are sometimes obliged to work under significant stress. This can often result in heightened error rates, including the performance of incorrect procedures. Other consequences of such resource constraints include systems designed, implemented and operated in an overly casual manner or 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 is still a process that 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 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 must be rigorously protected.

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.

6 Practical action plan for implementing ISO/IEC 27002

6.1 Taxonomy of the ISO/IEC 27002 and ISO/IEC 27001 standards

ISO/IEC 27002 provides a standard checklist of control objectives in 11 areas containing a total of 39 main security categories, each with a description of one or more security controls. Implementers of ISO/IEC 27002 in health environments will find that most of the control objectives apply in almost all situations. However, users of the standards in healthcare also need to recognise 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 ongoing compliance with ISO/IEC 27002 can best be ensured by the implementation of a management system as depicted in Figure 1.

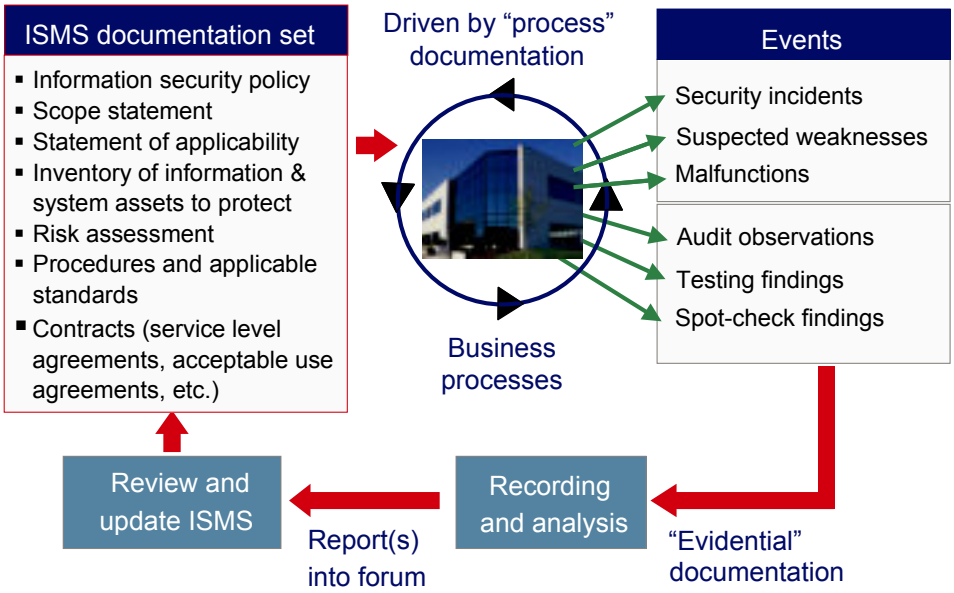

Figure 1 — The Information Security Management System

Health organizations should, where possible, integrate their ISMS with the information governance processes described in 5.2 and 5.3, and take account of the guidance given in 6.2 to 6.7.

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 adopting 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. See also 7.12.

6.2 Management commitment to implementing ISO/IEC 27002

It is essential that a health organization have the evident support of management before trying to achieve compliance with ISO/IEC 27002. Clearly, 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, 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 must be clearly shown.

Without these steps being taken, the commitment of others will be less than complete. Unnecessary suspicions can be aroused amongst stakeholders about the "real purpose" of the programme (e.g. is it to increase the effectiveness of information security or reduce the number of employees needed?).

Furthermore, management must be prepared for the likelihood that the short-term increase in expenditure arising from transition to the new regime is likely, especially in health, to produce negative comment. Such comments may also arise from a mixture of perceptions about the purposes and plans involved. Management's clear dedication can minimize such problems.

6.3 Establishing, operating, maintaining and improving the ISMS

Subclauses 6.4 to 6.7 provide guidance on establishing and then operating an ISMS in a health environment. This requires pursuing a cycle of activities, as illustrated in Figure 2.

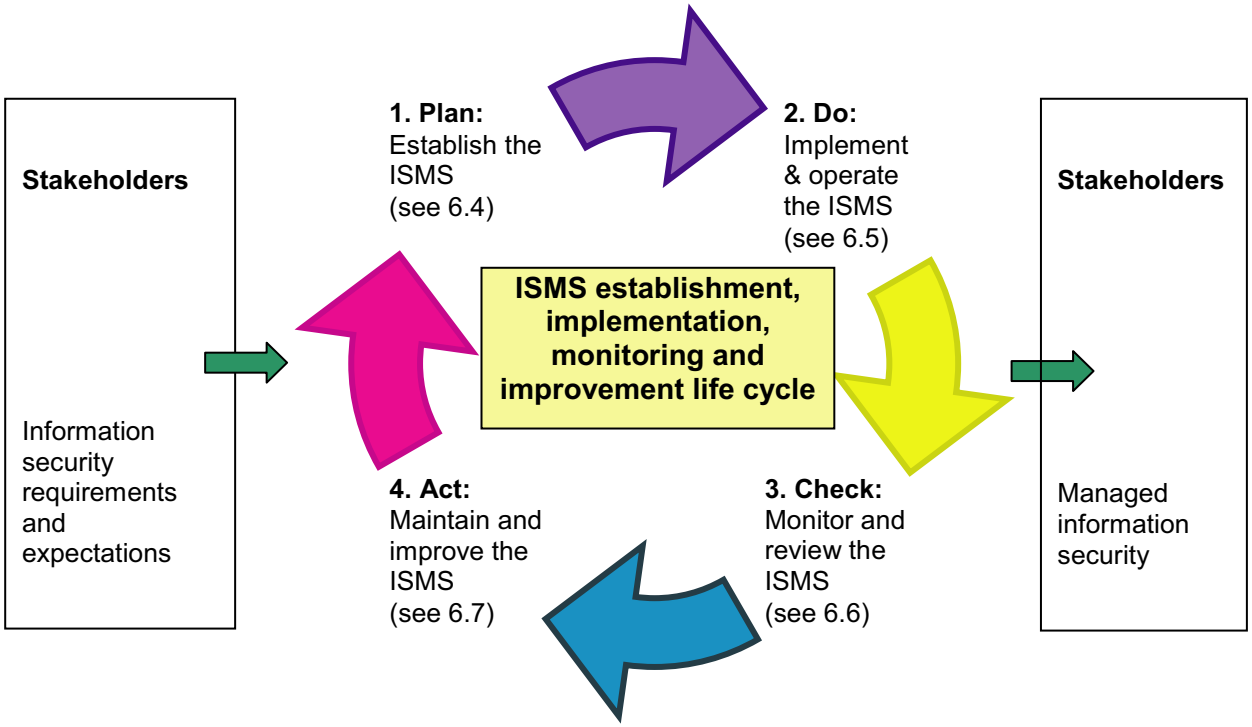

Figure 2 — ISMS process overview

Annex B gives informative examples of the steps typically involved in each phase of the life cycle, together with examples of the types of documents related to each phase.

6.4 Planning: establishing the ISMS

6.4.1 Selecting and defining a compliance scope

6.4.1.1 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.

Compliance scopes that cover no more than two to three sites or approximately 50 staff or approximately ten processes have been found to work very well. For this reason, primary care practices, clinics, home visit teams, hospital specialties and directorates, etc., all make effective scopes. An incremental and iterative process is thus 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.

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.

6.4.1.2 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 are typically "soft" in nature and cover such topics as:

a) the degree of visibility sought;

b) the balance of business and technical involvement intended;

c) the degree of local or central relevance sought;

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

6.4.1.3 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 gap analysis on a sampling basis to therefore 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.

6.4.1.4 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.

6.4.1.5 Service Level Agreements (SLAs) and contracts help establish the scope

SLAs and contracts can also assist in defining scope inasmuch 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.

6.4.1.6 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 7.3.2.1 for minimum requirements relating to scope statements.

6.4.2 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, documentation of security practices and evidence used to support the analysis. This is clearly 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 taken to interview 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 (see 6.4.5.1) and risk treatment (see 6.4.5.2). Also, gap analysis can suggest an initial priority rating for such improvements.

6.4.3 Establishing or enhancing a health information security forum

At the heart of the ISMS, an appropriate Information Security Management Forum (ISMF) must 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 organization’s (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.

As described in 5.2 and 5.3, the central nature of information security within information governance makes the positioning of the ISMF within the information governance structure a very sensible arrangement, but only if the latter group is, in turn, linked into 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. can only help to remove duplicated costs and to provide enhanced assurance of process integrity.

6.4.4 Assessing risks to health information

6.4.4.1 General

Risk assessment is the mechanism by which the controls framework that delivers the ISO/IEC 27002 control objectives is to be identified. This process is well documented in ISO/IEC/TR 13335-3.

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

6.4.4.2 Role of information security risk assessment in healthcare

Healthcare clearly 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.

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, e.g. guidelines recognising the importance of patient safety, uninterrupted availability of emergency services, professional accreditation, and clinical regulation.

6.4.4.3 Features of risk assessment with healthcare examples and reference to ISO/IEC 13335

A risk is composed of a causal relationship between several risk sources. Figure 3 shows the relationship between risks and risk sources in ISO/IEC 13335, making it clear that a risk value is determined from the surrounding asset values, threats, and vulnerabilities.

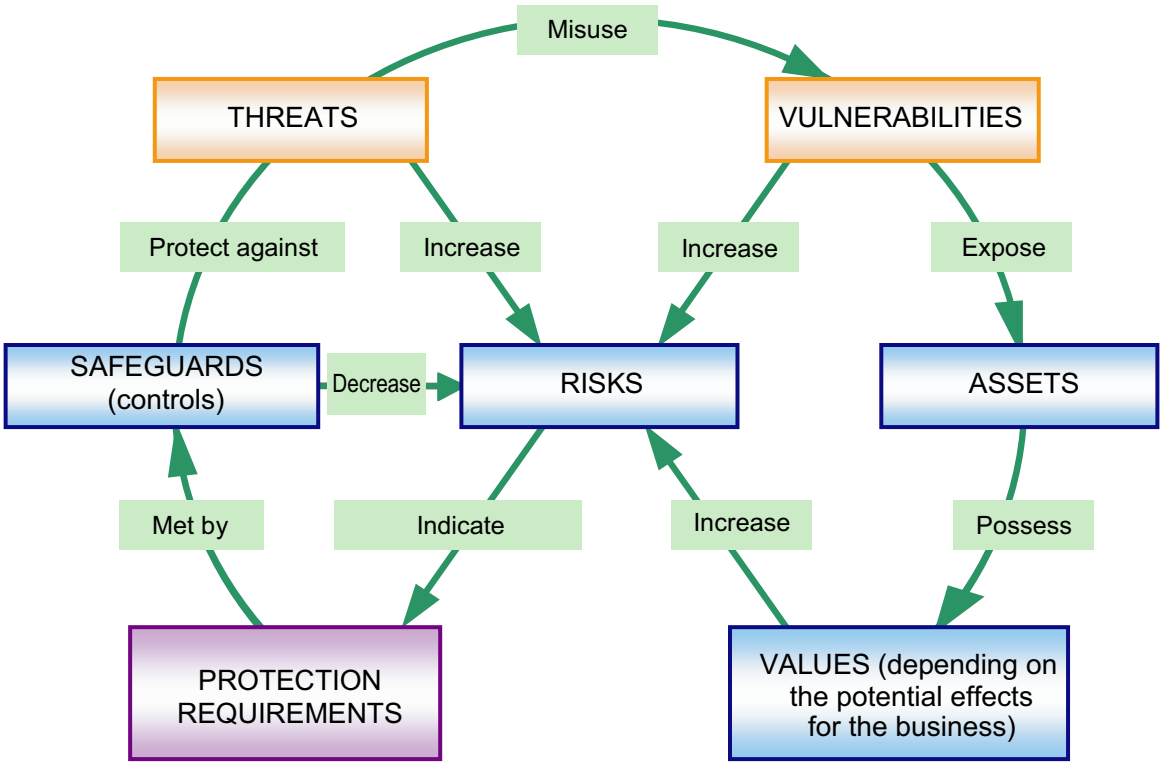

Figure 3 — Relationship between risks and risk sources in a simplified risk model

Information security risk assessment, and its subsequent management, is typically represented as in Figure 4.

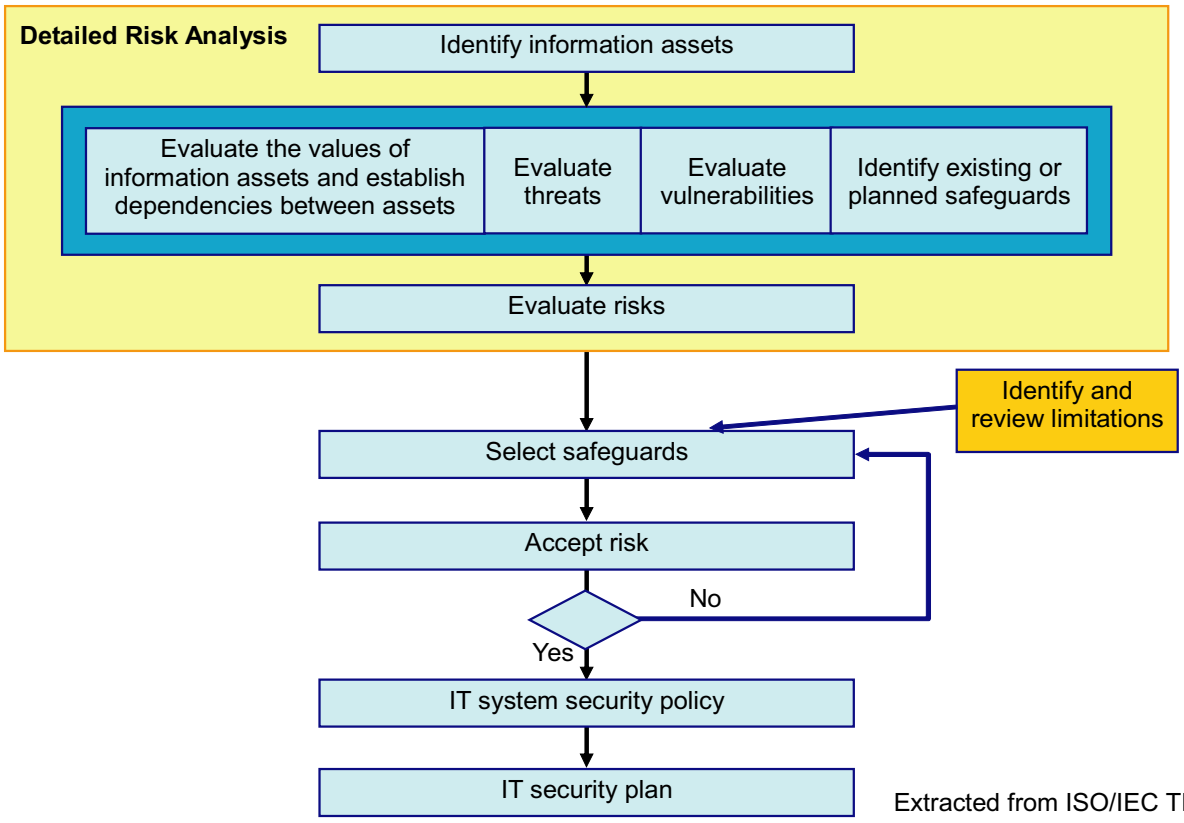

Figure 4 — Risk management using detailed risk analysis

Both ISO/IEC 27001 and ISO/IEC TR 13335-3 define the components of risk analysis and management as:

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 the 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 the light of the severe impact possible on health organizations, understanding these dependencies is essential.

6.4.4.4 Required skills and contributions

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. It is a reality that all individuals have different perspectives and different tolerances for risk. Challenges, even hypothetical and unlikely ones, are likely to be needed to get to the realistic "worst case scenarios" for impacts, threat likelihoods and vulnerabilities.

Naturally, actual past incidents are by default realistic but they may not be the worst case. Defining worst cases may well require specialist input. Scenarios with multiple "if" statements, however, are unlikely to be realistic. Health professionals are likely to benefit from the input of IT staff who will be able to identify failure modes and scenarios requiring assessment.

Effective information security risk assessment in healthcare requires the availability of the following skills and knowledge:

a) clinical and nursing process knowledge, including care protocols and pathways;

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

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

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

e) knowledge of incident histories and actual case impact scenarios;

f) detailed knowledge of systems architectures;

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

6.4.4.5 Required outputs

ISO/IEC TR 13335-3 defines the following typical outputs:

a) risk assessment report;

b) risk treatment plan.

Additionally, health organizations should also produce:

c) asset/dependency models (to support risk assessment);

d) status reports on controls;

e) risk treatment summary reports (to underpin gap analysis and the statement of applicability).

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.

6.4.5 Risk management

6.4.5.1 Risk assessment

Risk assessment is intended as a means to an end. It should not be 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 assessment by identifying which controls should 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 increasing 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.

6.4.5.2 Risk treatment

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.

6.4.5.3 Risk acceptance criteria

Health organizations need to define and document their criteria for the acceptance of risks. The factors to be taken into account are numerous and variable but the following should be considered for inclusion:

a) health sector, industry or organizational standards;

b) clinical or other priorities;

c) cultural fit;

d) reactions of subjects of care;

e) coherence with IT, clinical, and corporate risk acceptance strategy;

f) cost;

g) effectiveness;

h) type of protection;

i) number of threats covered;

j) risk level at which the controls become justified;

k) risk level that led to the recommendation being made;

l) alternatives already in place;

m) additional benefits derived.

Taken together, 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, not to implement a particular control is entirely valid but ought to be formally recorded for periodic review and re-assessment. Health organizations should document accepted risks.

6.4.5.4 Plans for handling outstanding areas of risk

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.

6.4.6 Security improvement planning

Authority for the security improvement plan should be taken, on behalf of 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 plans should be made available to clinical and other staff, as they are typically not a confidential document. Indeed, they can often be useful in demonstrating progress and process improvement.

Such plans will be most effective in minimizing interruptions to operations if they integrate information security improvements with planned changes in IT facilities and healthcare service provision. They also need to recognise known periods of unusual healthcare activity such as the influx of a new batch of interns or trainees.

6.4.7 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 organization'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 document should be provided to 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.

6.4.8 ISMS document set

The ISMS model shown in 6.1 lists the documentation required (see Figure 1). The essential documents are:

a) information security policy of the organization;

b) scope statement;

c) statement of applicability;

d) inventory of information assets and system assets to be protected;

e) risk assessment plans and reports;

f) procedures and standards agreed upon;

g) 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 facilitated 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.

Annex B contains the ISMS document set and related documents to the various steps in establishing or enhancing an ISMS.

6.4.9 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 re-used 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. Annex C contains an informative discussion of potential benefits and required attributes of such tools.

6.5 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 must 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 7 reviews each of the eleven security clauses of ISO/IEC 27002 and provides advice and guidance on the appropriate selection of security controls in a health environment.

d) **Training and educating:** 7.5.2.2 discusses the requirements for training and education for all staff, contractors, health professionals 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. Subclause 7.7 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. Subclause 7.10 contains a detailed discussion of security incident management.

6.6 Checking: monitoring and reviewing the ISMS

6.6.1 Need for ongoing assurance

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

A range of options is available for achieving that assurance. These options can be used in combinations. The less expensive options deliver commensurately less assurance, reflecting the limited rigour and independence they offer. Health organizations ought to create compliance auditing programmes that use a combination of technologies and approaches.

6.6.2 Compliance assessment

6.6.2.1 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.

6.6.2.2 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, e.g. between information security officers. However, this can of course mean that there could be an agreement for mutually positive reports.

6.6.2.3 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” inasmuch as the personnel involved are likely to have performed other such independent audits from which they can draw comparisons.

6.6.2.4 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 organizations 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, e.g. by initial agreement that the scope statement discussed in 6.4.1 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 days to 6 days effort by the certification auditor.

The ultimate independent audit is that provided under the guidelines of ISO 27001, as performed by a competent, independent auditing body such as is 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.

6.7 Acting: maintaining and improving the ISMS

Results of the monitoring activities described in 6.6 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 SOA described in 6.4.7 can be an effective tool for keeping those responsible for clinical and corporate governance apprised of the current state of the ISMS. The format used for the SOA 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 6.4.6 is also an important tool in demonstrating progress and process improvement.

7 Healthcare implications of ISO/IEC 27002

7.1 General

This clause contains specific advice on the eleven security control clauses and 39 main security control categories described in ISO/IEC 27002.

The general approach taken by ISO/IEC 27002 is to encourage each organization to consider and interpret that document within its own context and legal and business requirements. Yet experience gained in several countries including Australia, Canada, France, the Netherlands, New Zealand, South Africa, and the United Kingdom has shown the need for certain control clauses and control categories whenever personal health information is to be secured. Based on this experience, minimum requirements are stated where appropriate and, in a few cases, normative guidelines are set out describing the proper application of certain ISO/IEC 27002 security controls to the protection of health information. These minimum requirements are so essential to the protection of personal health information that any health organizations that do not meet them cannot be said to comply with this International Standard.

In every subclause that follows, the guidance given is in addition to, but not a replacement for, the guidance found in ISO/IEC 27002.

7.2 Information security policy

7.2.1 Information security policy document

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

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 6.4.1.6;

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.

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 documents 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:

f) the breadth of health information;

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

h) the rights of subjects of care, where applicable, to privacy and to access to their records;

i) the obligations of clinicians with respect to obtaining informational consent from subjects of care and maintaining the confidentiality of personal health information;

j) 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;

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

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

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

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

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.

7.2.2 Review of the information security policy document

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

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).

7.3 Organizing information security

7.3.1 General

A health organization's management is responsible for the security of personal health information and other protected health-related data processed by the organization. This is especially worth noting for organizations that rely upon managed services provided by third parties. Effective coordination is also an essential ingredient in maintaining information security. Both require an explicit and robust information security management infrastructure.

7.3.2 Internal organization

7.3.2.1 Management commitment to information security, information security coordination and allocation of information security responsibilities

Control

Organizations processing personal health information **shall**:

a) clearly define and assign information security responsibilities;

b) have an 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 6.4.3.

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

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 6.2. 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 6.4.3, 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.

7.3.2.2 Authorization process for information processing facilities

No additional guidance for information security management in health.

7.3.2.3 Confidentiality agreements

Control

In addition to following the guidance 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

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

7.3.2.4 Contact with authorities, contact with special interest groups, and independent review of information security

No additional guidance for information security management in health.

7.3.3 Third parties

7.3.3.1 Identification of risks related to external parties

Control

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

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 must 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.

7.3.3.2 Addressing security when dealing with customers

No additional guidance for information security management in health.

7.3.3.3 Addressing security in third-party agreements

Control

Health organizations using the services of third parties, where the services of those parties process personal health information, **shall** employ formal contracts that specify:

a) the confidential nature and value of the personal health information;

b) the security measures to be implemented and/or complied with;

c) limitations to access to these services by third parties;

d) the service levels to be achieved in the services provided;

e) the format and frequency of reporting to the health organization's ISMF;

f) the arrangement for representation of the third party in appropriate health organization meetings and working groups;

g) the arrangements for compliance auditing of the third parties;

h) the penalties exacted in the event of any failure in respect of the above.

Implementation guidance

In addition to the guidance given by ISO/IEC 27002, the requirement above is intended to ensure that the confidentiality, integrity and availability of personal health information is maintained as the information flows beyond the direct control of a health organization. Where that flow crosses jurisdictional boundaries, additional guidance can be found in ISO 22857.

Where a third party is not processing personal health information, an appropriate subset of the contract features above may still be appropriate. In all cases of third-party service provision, an agreement that specifies the minimum set of controls to be applied should be adopted.

7.4 Asset management

7.4.1 Responsibility for health information assets

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;

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

Implementation guidance

Organizations processing health information **should** have rules for maintaining the currency of these 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.

7.4.2 Health information classification

7.4.2.1 Classification guidelines

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

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 must 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 emphasise 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 7.5.2.1.

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, i.e. 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.

7.4.2.2 Information labelling and handling

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

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.

7.5 Human resources security

7.5.1 Prior to employment

7.5.1.1 Roles and responsibilities

Implementation guidance

In addition to following the guidance 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.

7.5.1.2 Screening

Control

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.

Implementation guidance

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, e.g. by professional bodies and academic institutions.

Wherever possible, criminal background checks **should** be undertaken. See also 7.8.2.1.

7.5.1.3 Terms and conditions of employment

Implementation guidance

In addition to following the guidance given by ISO/IEC 27002, all organizations that process personal health information **should** include in the terms and conditions of employment of employees who process, or will process, personal health information a statement about the employee's responsibility for information security.

The terms and conditions of employment **should**:

a) include reference to the penalties that are possible when breach of the information security policy is identified;

b) ensure that conditions relating to confidentiality of personal health information survive the completion of the employment in perpetuity.

With respect to clinical staff, the terms and conditions of employment **should** specify what rights of access such staff will have to the records of subjects of care and to the associated health information systems in the event of third-party claims.

If there has been a long gap between recruitment and the date of the employee starting, serious consideration **should** be given to repeating the screening process, or key elements of it.

7.5.2 During employment

7.5.2.1 Management responsibilities

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.

7.5.2.2 Information security awareness, education and training

Control

In addition to following the guidance 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.

7.5.2.3 Disciplinary process

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.

7.5.3 Termination or change of employment

7.5.3.1 Termination responsibilities and return of assets

Implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note that in healthcare, many types of staff, e.g. 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.

7.5.3.2 Removal of access rights

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

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.

7.6 Physical and environmental security

7.6.1 Secure areas

7.6.1.1 Physical security perimeter

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

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.

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.

7.6.1.2 Physical entry controls; securing offices, rooms and facilities; protecting against external and environmental threats; working in secure areas

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.

7.6.1.3 Public access, delivery and loading areas

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.

7.6.2 Equipment security

7.6.2.1 Equipment siting and protection

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.

7.6.2.2 Supporting utilities, cabling security and equipment maintenance

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.

7.6.2.3 Security of equipment off-premises

Control

In addition to following the guidance 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.)

7.6.2.4 Secure disposal or re-use of equipment

Control

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

7.6.2.5 Removal of property

Control

In addition to following the guidance 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.

7.7 Communications and operations management

7.7.1 Operational procedures and responsibilities

7.7.1.1 Documented operating procedures

No additional guidance for information security management in health.

7.7.1.2 Change management

Control

In addition to following the guidance 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

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.

7.7.1.3 Segregation of duties

Implementation guidance

In addition to following the guidance 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.

Organizations processing personal health information **should** ensure that the IT systems employed contain application functionalities that enforce the approval of clinical processes by different role holders, where this is required.

7.7.1.4 Separation of development, test and operational facilities

Control

In addition to following the guidance 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).

7.7.2 Third-party service delivery management

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.

7.7.3 System planning and acceptance

7.7.3.1 Capacity management

No additional guidance for information security management in health.

7.7.3.2 System acceptance

Control

In addition to following the guidance 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.

Implementation guidance

The extent and rigour of those tests **should** be scaled to a level consistent with the identified risks of the change. See also 7.7.1.2.

7.7.4 Protection against malicious and mobile code

7.7.4.1 Controls against malicious code

Control

In addition to following the guidance 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.

7.7.4.2 Controls against mobile code

No additional guidance for information security management in health.

7.7.5 Health information backup

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.

7.7.6 Network security management

7.7.6.1 Network controls

No additional guidance for information security management in health.

7.7.6.2 Security of network services

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 7.11.

7.7.7 Media handling

7.7.7.1 Management of removable computer media

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.

7.7.7.2 Disposal of media

Control

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

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.

7.7.7.3 Information handling procedures

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.

7.7.7.4 Security of system documentation

No additional guidance for information security management in health.

7.7.8 Exchanges of information

7.7.8.1 Health information exchange policies and procedures and exchange agreements

Implementation guidance

In addition to the guidance given by ISO/IEC 27002, 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.

Organizations **shall** ensure that the security of such exchanges of information is the subject of policy development and compliance audit (see 7.12).

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.

7.7.8.2 Physical media in transit

No additional guidance for information security management in health.

7.7.8.3 Electronic messaging

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 the Bibliography for a list of standards related to the use of digital certificates in health environments.

See also 7.12.2.2 for a discussion of consent prior to communication outside the organization.

7.7.8.4 Health information systems

No additional guidance for information security management in health.

7.7.9 Electronic health information services

7.7.9.1 Electronic commerce and online transactions

Implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note the care that must 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.

7.7.9.2 Publicly available health information

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.

7.7.10 Monitoring

7.7.10.1 General

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.

7.7.10.2 Audit logging

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.

7.7.10.3 Monitoring system use

Implementation guidance

In addition to following the guidance given by ISO/IEC 27002, 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.

7.7.10.4 Protection of log information

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

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.

7.7.10.5 Administrator and operator logs

No additional guidance for information security management in health.

7.7.10.6 Fault logging

No additional guidance for information security management in health.

7.7.10.7 Clock synchronization

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

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.

7.8 Access control

7.8.1 Requirements for access control in health

7.8.1.1 General

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.

7.8.1.2 Access control policy

Control

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 7.2.1, **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.

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.

7.8.2 User access management

7.8.2.1 User registration

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

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. via 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 7.5.1.2.

7.8.2.2 Privilege management

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).

Implementation guidance

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/TS 22600-1 and in ISO/TS 22600-2.

7.8.2.3 User password management

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.

7.8.2.4 Review of user access rights

Implementation guidance

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.

7.8.3 User responsibilities

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.

7.8.4 Network access control and operating system access control

No additional guidance for information security management in health.

7.8.5 Application and information access control

7.8.5.1 Information access restriction

Control

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

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.

7.8.5.2 Sensitive system isolation

No additional guidance for information security management in health.

7.8.6 Mobile computing and teleworking

7.8.6.1 Mobile computing and communications

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 in healthcare mobile computing;

b) prepare policy on the precautions to be taken when using mobile computing devices, including wireless devices;

c) require their mobile users to follow 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).

7.8.6.2 Teleworking

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. See also 7.7.7.1 and 7.7.8.3.

7.9 Information systems acquisition, development and maintenance

7.9.1 Security requirements of information systems

No additional guidance for information security management in health.

7.9.2 Correct processing in applications

7.9.2.1 Uniquely identifying subjects of care

Control

Health information systems processing personal health information **shall**:

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

b) 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.

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 must 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.

7.9.2.2 Input data validation

No additional guidance for information security management in health.

7.9.2.3 Control of internal processing

No additional guidance for information security management in health.

7.9.2.4 Message integrity

No additional guidance for information security management in health.

7.9.2.5 Output data validation

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.

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”).

7.9.3 Cryptographic controls

7.9.3.1 Policy on the use of cryptographic controls and key management

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.

7.9.3.2 Key management

No additional guidance for information security management in health.

7.9.4 Security of system files

7.9.4.1 Control of operational software

No additional guidance for information security management in health.

7.9.4.2 Protection of system test data

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.

7.9.4.3 Access control to program source code

No additional guidance for information security management in health.

7.9.5 Security in development and support processes, and technical vulnerability management

No additional guidance for information security management in health.

7.10 Information security incident management

7.10.1 Reporting information security events and weaknesses

Implementation guidance

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 a quick, effective and orderly response to security incidents;

b) to ensure that there is an effective 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 data such as audit trails, logs and other 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.

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.

7.10.2 Management of incidents and improvements

7.10.2.1 Responsibilities and procedures

No additional guidance for information security management in health.

7.10.2.2 Learning from incidents

No additional guidance for information security management in health.

7.10.2.3 Collection of evidence

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 interjurisdictional requirements when health information systems are accessible across jurisdictional boundaries.

7.11 Information security aspects of business continuity management

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 need to ensure that their business continuity management planning includes health crisis management planning.

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.

7.12 Compliance

7.12.1 General

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, i.e. 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 Internatioanal 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.

7.12.2 Compliance with legal requirements

7.12.2.1 Identification of applicable legislation, intellectual property rights and protection of organizational records

No additional guidance for information security management in health.

7.12.2.2 Data protection and privacy of personal information

Control

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, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organization.

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:*
>
> *i. to his/her health*
>
> *ii. 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.

7.12.2.3 Prevention of misuse of information-processing facilities and regulation of cryptographic controls

No additional guidance for information security management in health.

7.12.3 Compliance with security policies and standards and technical compliance

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.

7.12.4 Information systems audit considerations in a health environment

No additional guidance for information security management in health.

Annex A
(informative)

Threats to health information security

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

1) 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 of covering up cases where harm has been caused.

2) 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 unauthorized 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.

3) Masquerade by outsiders (including hackers)

Masquerade by outsiders occurs when unauthorized third parties gain access to system data or resources, either by impersonating an authorized user or by fraudulently becoming an authorized 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:

i) user identification;

ii) user authentication;

iii) origin authentication;

iv) access control and privilege management.

4) Unauthorized use of a health information application

It can be surprisingly easy to obtain unauthorized 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 *un*authorized 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 must be rigorously protected.

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

i) 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);

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

iii) personnel security (e.g., by providing inadequate training to users or not making clear that their access to records is subject to audit and review).

5) 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 e-mail 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.

6) 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 on to 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 systems 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.

7) 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).

8) 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 e-mails during transmission. Hacker tools are readily available to automate and simplify much of this process. Communications interception constitutes a failure in secure communications.

9) 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). Establishing unambiguously whether personal health information flowed from one health provider 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 e-mail messages (an example of repudiation of receipt).

10) 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 via fax or over the Internet.

11) Embedding of malicious code

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

12) 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 providers (or both).

13) 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 Clause 10 of ISO/IEC 27002:2005. While in no way unique to health information systems, the loss of availability of such systems can have life-threatening consequences for patients.

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

Health information systems can be critical during natural disasters and other events that can be life-threatening to large numbers of people. These same disasters can wreak 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.

15) 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.

16) 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.

17) Operator error

Operator error accounts form 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:

i) operations controls;

ii) personnel security (including effective training);

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

18) 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.

19) 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:

i) user controls (including user interfaces designed with security in mind) or

ii) personnel security (including training).

20) 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 jeopardises the availability of such systems. A failure of this kind constitutes a failure in business continuity management (see Clause 14 of ISO/IEC 27002:2005).

21) 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 their 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.

22) 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 reside on a server or laptop computer that is stolen or else because the data themselves are 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.

23) 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 Clause 8 of ISO/IEC 27002:2005).

24) 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, acts of this kind constitute a failure to effectively 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 Clause 9 of ISO/IEC 27002:2005 need to be carefully selected and applied to minimize such threats.

25) Terrorism

The threat of terrorism includes acts by extremist groups wishing to damage or disrupt the work of health organizations or to harm healthcare providers 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)

Tasks and related documents of the Information Security Management System

B.1 Tasks and related documents for establishing the ISMS (Plan)

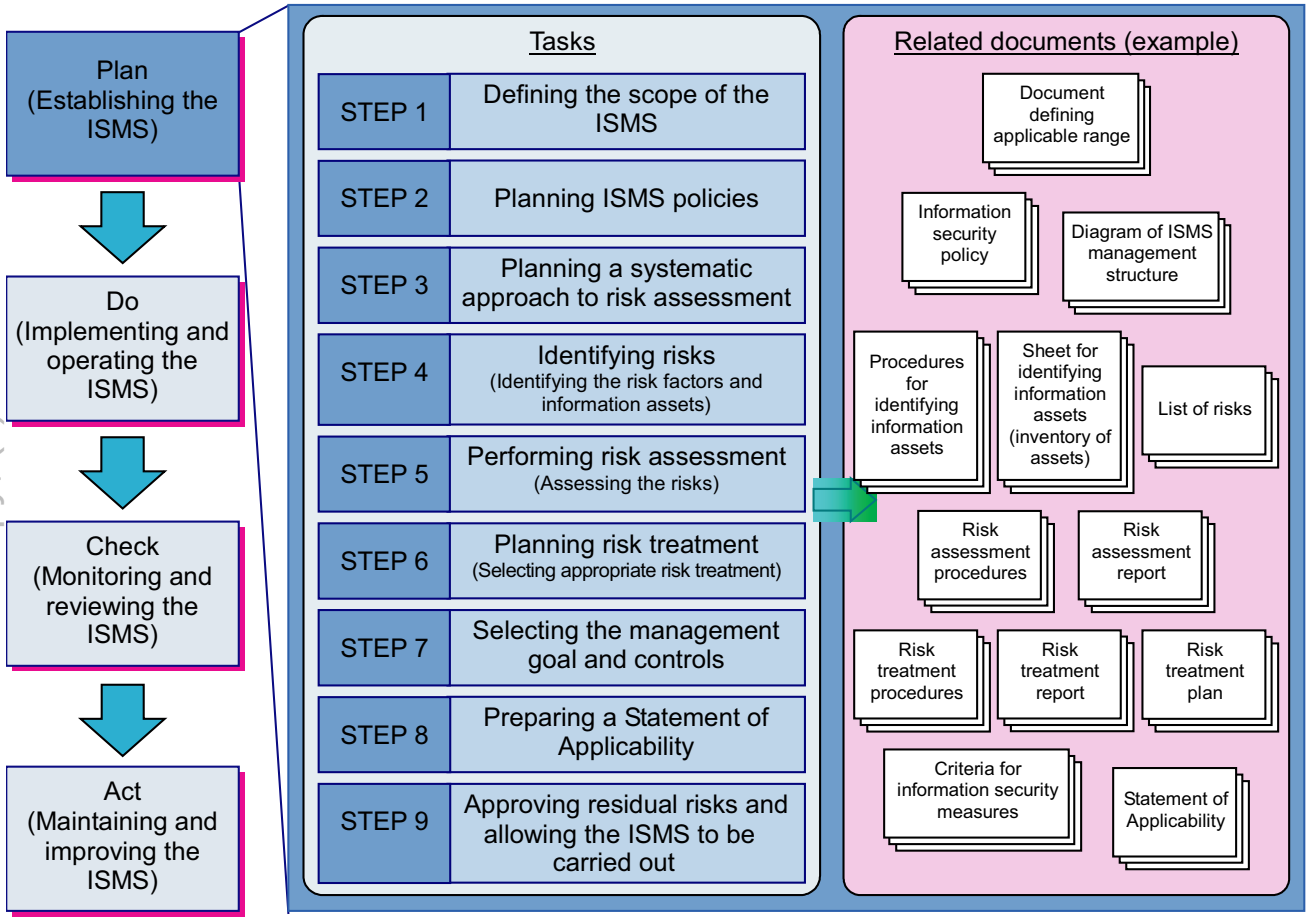

Figure B.1 — Tasks and related documents for establishing the ISMS

B.2 Tasks and related documents for implementing and operating the ISMS (Do)

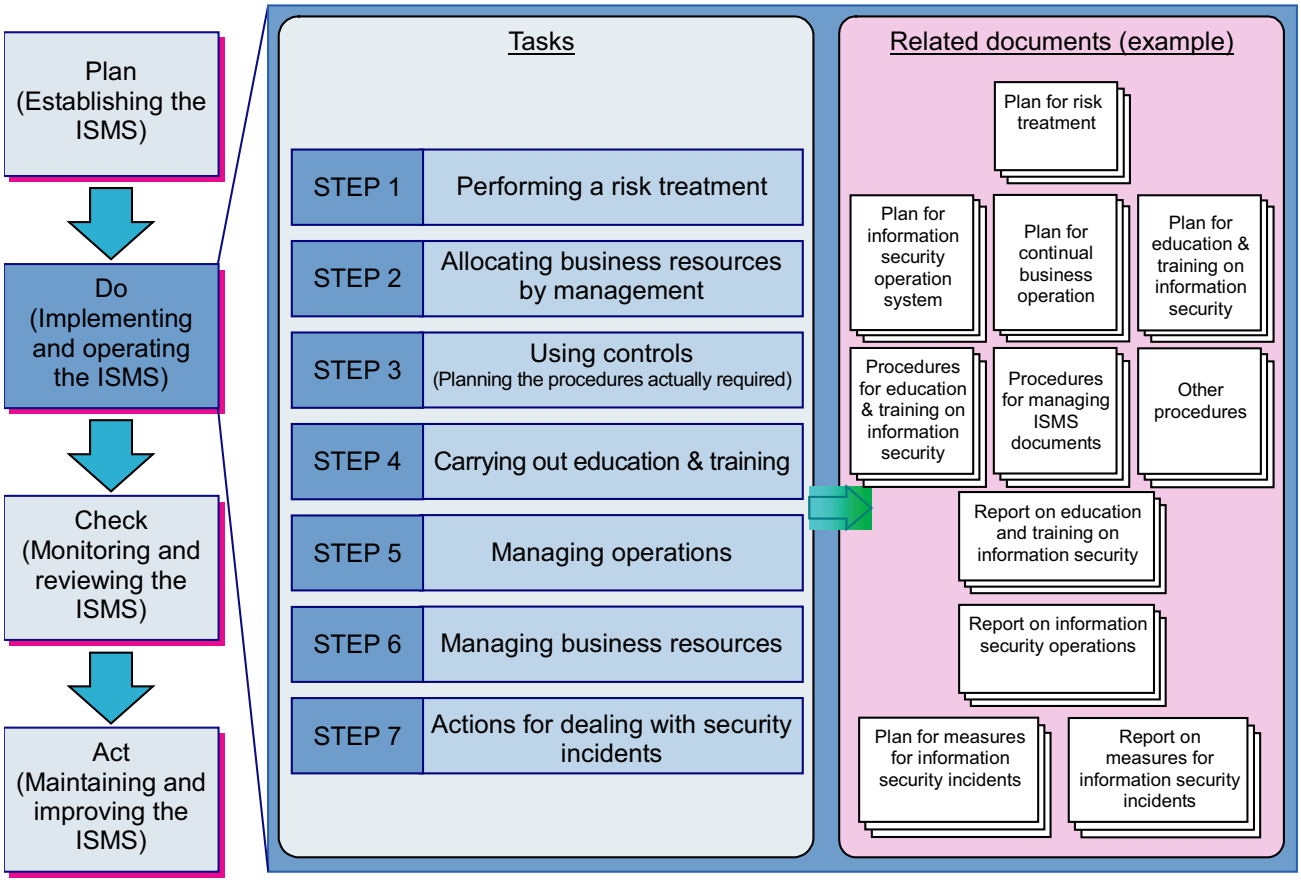

Figure B.2 — Tasks and related documents for implementing and operating the ISMS

B.3 Tasks and related documents for monitoring and reviewing the ISMS (Check)

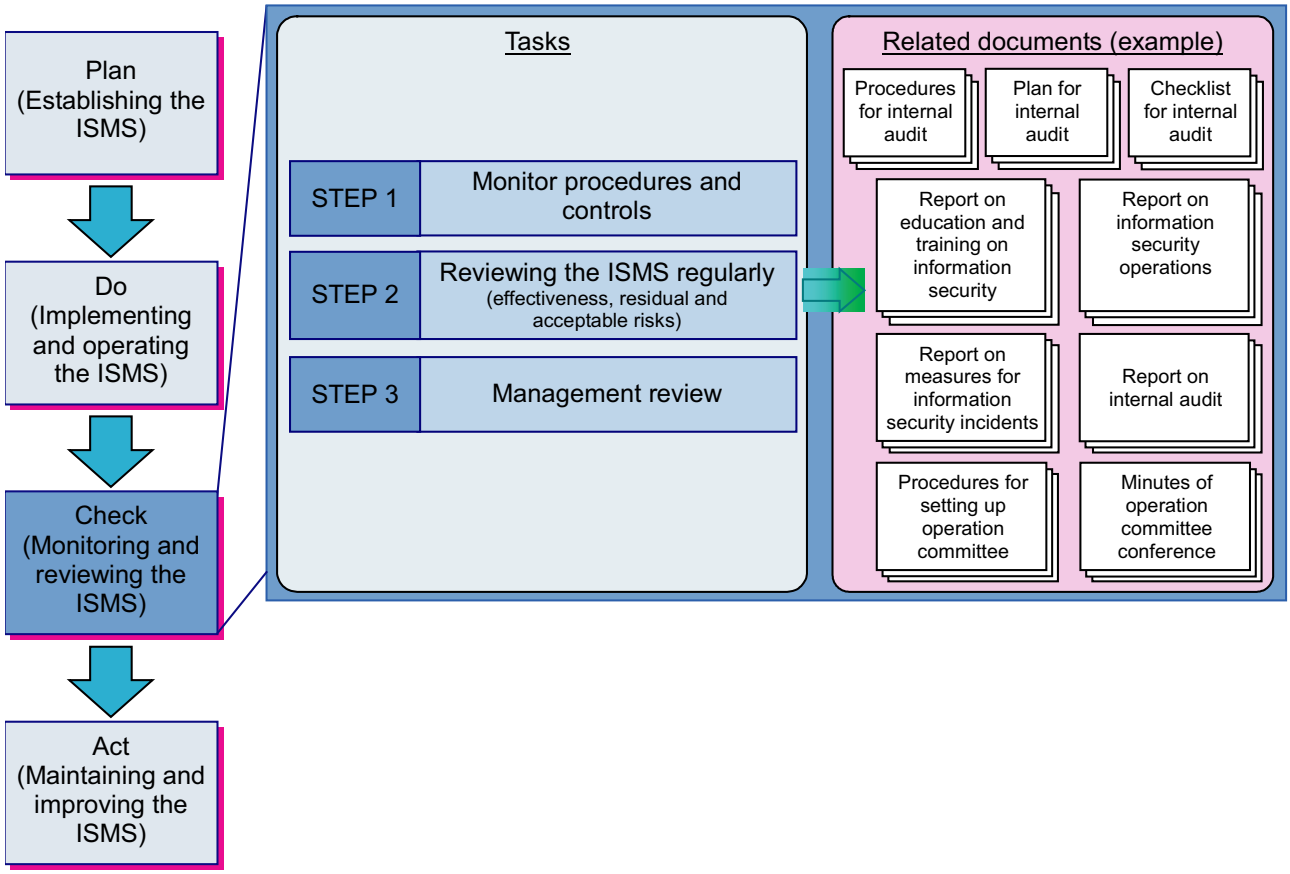

Figure B.3 — Tasks and related documents for monitoring and reviewing the ISMS

B.4 Tasks and related documents for maintaining and improving the ISMS (Act)

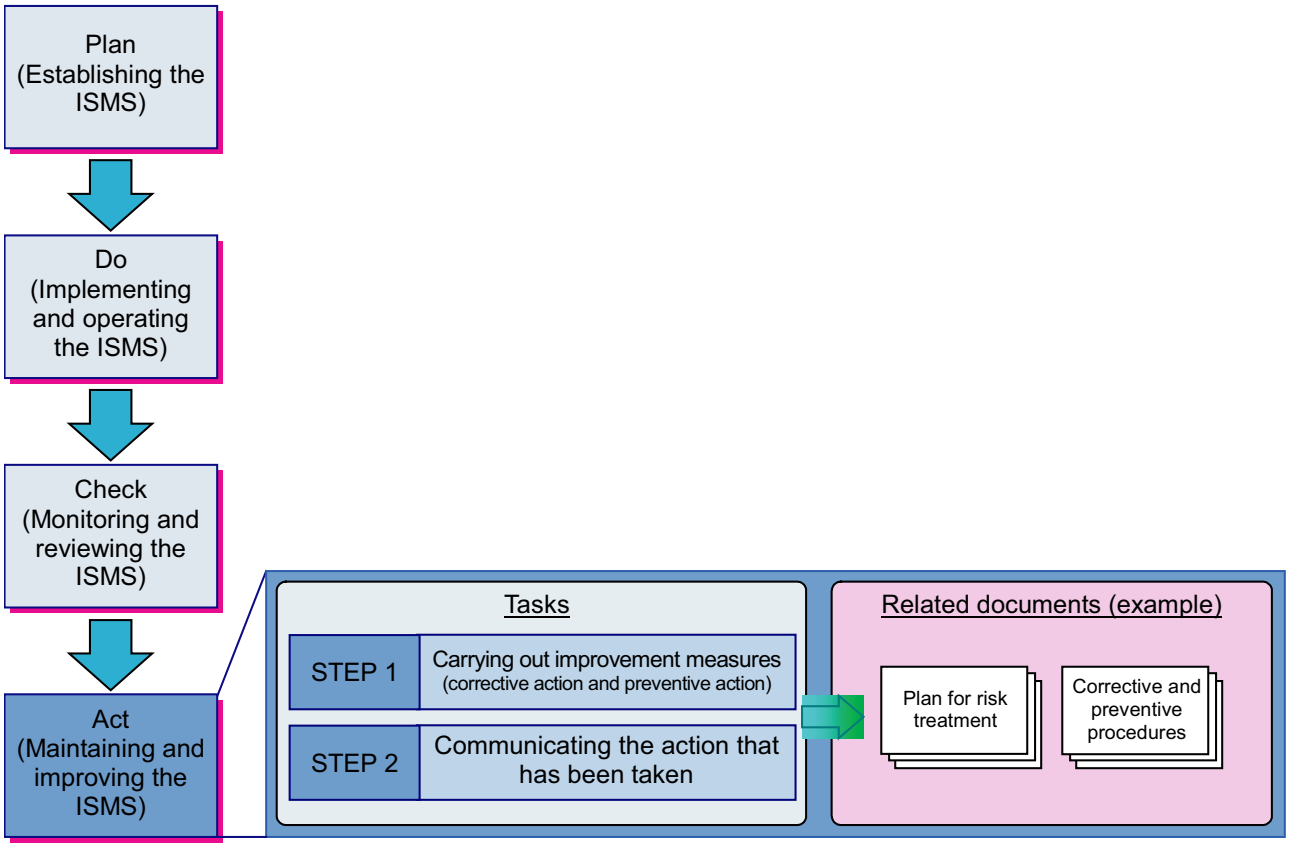

Figure B.4 — Tasks and related documents for maintaining and improving the ISMS

Annex C
(informative)

Potential benefits and required attributes of support tools

C.1 Potential benefits of support tools

Although database tools are by no means mandatory, evidence has repeatedly 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 maximize compliance while minimizing 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.

The potential benefits of tool support are:

a) simplified data entry and data maintenance;

b) pre-formatted reports and other outputs;

c) simplified version control;

d) optimized data re-use within the process;

e) consistency of approach;

f) re-usability of data and results in subsequent exercises;

g) comparability of results;

h) completeness of approach;

i) confidence of third parties, especially auditors;

j) visibility of the implications of decisions;

k) decision support and other management processes;

l) capacity to undertake searches and interrogations;

m) significantly reduced human resource costs;

n) relatively easy transfer of material to successors.

C.2 Required attributes of support tools

The required attributes of such tools are:

a) reputable manufacturer;

b) availability of support and training;

c) content maintenance in line with changes in the standard;

d) effective integration with other office productivity tools;

e) effective integration with the operating system;

f) an effective and intuitive, typically graphical or Web, interface;

g) (ideally) ability to customize the content and output;

h) (ideally) a multi-user support process.

C.3 Tool support for ISO/IEC 27002 process

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

a) scoping and scope statement production;

b) gap analysis and gap analysis reporting;

c) asset definition and asset inventory reporting;

d) secure improvement plan production, reporting and implementation status recording;

e) statement of applicability recording and reporting;

f) security resource definition and reporting.

It is worth noting that all the above processes interact and need to be able to interoperate.

C.4 Tool support for risk analysis process

The risk analysis and management functionality that can be supported by tools encompass all the minimum processes defined in Clause C.3. However, the more advanced tools additionally provide one or more of the following:

a) risk model library support;

b) asset libraries;

c) asset valuation tools;

d) dependency modelling support;

e) asset grouping for assessment efficiency;

f) threat/asset/impact mappings for high integrity within the assessments;

g) multiple levels of threat and vulnerability assessment to meet different needs;

h) countermeasure libraries;

i) prioritization functionality;

j) costing and time scaling of improvements;

k) security documentation support;

l) decision support functions;

m) auditing support;

n) risk treatment reporting;

o) “What If?” functionality;

p) graphical reports.

Again, it is worth noting that many of the above processes interact and need to be able to interoperate.

Bibliography

Related standards in health information security

Implementers of digital certificates or digital signatures in healthcare are referred to:

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

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

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

Those responsible for national, provincial, territorial, or state-wide health information infrastructures, who wish to ensure that health information security is maintained as health information flows across jurisdictional boundaries, are referred to:

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

Indeed, any organization involved in the transfer of personal health information to another organization would benefit from reading the above-mentioned standard.

Designers and implementers of privilege management infrastructures are refer to:

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

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

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

[8] ISO/TS 21298, *Health informatics — functional and structural roles*

Designers and implementers of health provider directories are referred to:

[9] ISO/TS 21091, *Health informatics — Directory services for security, communications and identification of professionals and patients*

Designers and implementers of information systems that provide for the anonymization or pseudonymization of personal health information are referred to:

[10] ISO/TS 25237, *Health informatics — Pseudonymisation*

Other standards

[11] ISO/TR 18307, *Health informatics — Interoperability and compatibility in messaging and communication standards — Key characteristics*

[12] ISO/TS 18308, *Health informatics — Requirements for an electronic health record architecture*

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

[14] ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

[15] ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*

[16] ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*

[17] ISO/IEC 13335-1, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

[18] ISO/IEC TR 13335-3, *Information technology — Guidelines for the management of IT Security — Part 3: Techniques for the management of IT security*

[19] ISO/IEC TR 13335-4, *Information technology — Guidelines for the management of IT Security — Part 4: Selection of safeguards*

[20] ISO/IEC TR 13335-5, *Information technology — Guidelines for the management of IT Security — Part 5: Management guidance on network security*

[21] ISO/TR 20514, *Health informatics — Electronic health record — Definition, scope and context*

[22] Australian Standard HB 174:2003, *Information security management — Implementation guide for the health sector*

[23] Australian Standard HB 231:2000, *Information security risk management guidelines*

[24] AS/NZS 4360, *Risk management*

[25] Canada Health Infoway Electronic Health Record Privacy and Security Requirements, **v. 1.1**, 2005

[26] Japan Information Processing Development Corporation JIP-ISMS-114-1.0, *ISMS Users Guide for Medical Organizations — Guidance on the Application of ISMS Certification Criteria* (Version 2.0)

[27] ISO 7498-2, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[28] ISO/IEC Guide 73, *Risk management — Vocabulary — Guidelines for use in standards*

BSI - British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001. Fax: +44 (0)20 8996 7001 Email: orders@bsigroup.com You may also buy directly using a debit/credit card from the BSI Shop on the Website http://www.bsigroup.com/shop

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact Information Centre. Tel: +44 (0)20 8996 7111 Fax: +44 (0)20 8996 7048 Email: info@bsigroup.com

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001 Email: membership@bsigroup.com

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsigroup.com/BSOL

Further information about BSI is available on the BSI website at http://www.bsigroup.com.

Copyright

BSI Group
Headquarters 389
Chiswick High Road,
London, W4 4AL, UK
Tel +44 (0)20 8996 9001
Fax +44 (0)20 8996 7001
www.bsigroup.com/
standards