INTERNATIONAL STANDARD

ISO 27799

First edition
2008-07-01

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

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

Reference number
ISO 27799:2008(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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.

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.