SLOVENSKI STANDARD
oSIST prEN ISO 27799:2014

01-november-2014

Zdravstvena informatika - Upravljanje informacijske varnosti v zdravstvu z uporabo standarda ISO/IEC 27002 (ISO/DIS 27799:2014)

Health informatics - Information security management in health using ISO/IEC 27002 (ISO/DIS 27799:2014)

Medizinische Informatik - Informationsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 (ISO/DIS 27799:2014)

Informatique de santé - Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002 (ISO/DIS 27799:2014)

Ta slovenski standard je istoveten z: **prEN ISO 27799**

ICS:

35.240.80	Uporabniške rešitve IT v zdravstveni tehniki	IT applications in health care technology

oSIST prEN ISO 27799:2014 **en,fr,de**

DRAFT INTERNATIONAL STANDARD

ISO/DIS 27799

ISO/TC **215**

Secretariat: **ANSI**

Voting begins on:
2014-09-11

Voting terminates on:
2015-02-11

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

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

ICS: 35.240.80

ISO/CEN PARALLEL PROCESSING

This draft has been developed within the International Organization for Standardization (ISO), and processed under the **ISO lead** mode of collaboration as defined in the Vienna Agreement.

This draft is hereby submitted to the ISO member bodies and to the CEN member bodies for a parallel five month enquiry.

Should this draft be accepted, a final draft, established on the basis of comments received, will be submitted to a parallel two-month approval vote in ISO and formal vote in CEN.

To expedite distribution, this document is circulated as received from the committee secretariat. ISO Central Secretariat work of editing and text composition will be undertaken at publication stage.

Reference number
ISO/DIS 27799:2014(E)

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*, Subcommittee SC , .

This second/third/... edition cancels and replaces the first/second/... edition (ISO 27799:2008), [clause(s) / subclause(s) / table(s) / figure(s) / annex(es)] of which [has / have] been technically revised.

Introduction

This international standard provides guidance to healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information. It is based upon—and extends—the general guidance provided by ISO/IEC 27002 *Information technology — Security techniques —Code of practice for information security controls* [1] and addresses the special information security management needs of the health sector and its unique operating environments. While the protection and security of personal information is important to all individuals, corporations, institutions and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, auditability and availability of personal health information. This type of information is regarded by many as being among the most confidential of all types of personal information. Protecting this confidentiality is essential if the privacy of subjects of care is to be maintained. The integrity of health information 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.

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

ISO/IEC 27002 is already being used extensively for health informatics IT security management through the agency of national or regional guidelines in Australia, Canada, France, the Netherlands, New Zealand, South Africa, the United Kingdom and elsewhere. The present 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 the ISO/IEC 27000 series of standards. Rather, it is a complement to these more generic standards.

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

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

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

[1] This guideline is consistent with the revised version of ISO/IEC 27002:2013.

Objectives

Maintaining information confidentiality, availability, and integrity (including authenticity, accountability and auditability) are the overarching goals of information security. In healthcare, privacy of subjects of care depends upon maintaining the confidentiality of personal health information. To maintain confidentiality, measures 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 this standard are those identified as appropriate in healthcare to protect confidentiality, integrity and availability of personal health information and to ensure that access to such information can be audited and accounted for. These controls help to prevent errors in medical practice that might ensue from failure to maintain the integrity of health information. In addition, they help to ensure that the continuity of medical services is maintained.

There are additional considerations that shape the goals of health information security. They include:

a) honouring legislative obligations as expressed in applicable data protection laws and regulations protecting a subject of care's right to privacy[2];

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; and

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

Relation to information governance,[3] corporate governance and clinical governance

While health organizations may differ in their positions on clinical governance and corporate governance, the importance of integrating and attending to information governance ought to be beyond debate as a vital

[2] 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, impact health information security policy.

[3] Note that in some countries, information governance is referred to as information assurance.

support to both. As health organizations have become ever more critically dependent on information systems to support care delivery (e.g. by exploiting decision support technologies and trends towards 'evidence based' rather than 'experience based' healthcare), it has become evident that events in which losses of integrity, availability and confidentiality occur may have a significant clinical impact and that problems arising from such impacts will be seen to represent failures in the ethical and legal obligations inherent in a 'duty of care'.

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

Health information to be protected

There are several types of information whose confidentiality, integrity and availability[4] need to be protected:

a) personal health information,

b) pseudonymised data derived from personal health information via some methodology for pseudonymous identification,

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

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

e) data on health professionals, staff and volunteers,

f) information related to public health surveillance,

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

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

The extent to which confidentiality, integrity and availability need to be protected depends upon the nature of the information, the uses to which it is put, and the risks to which it is exposed. For example, statistical data (item 3 above) may not be confidential, but protecting its integrity may be very important. Likewise, audit trail data (item 7 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 section ***). The results of regular risk assessment need to be fitted to the priorities and resources of the implementing organization.

Threats and vulnerabilities in health information security

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

By their nature, health organizations operate in an environment where visitors and the public at large can never be totally excluded. In large health organizations, the sheer volume of people moving through operational areas is significant. These factors increase the vulnerability of systems to physical threats. The

[4] Level of availability depends upon the uses to which the data will be put.

likelihood that such threats will occur may increase when emotional or mentally ill subjects of care or relatives are present.

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.

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

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

Who should read this standard?

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

This 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.

Benefits of using this standard

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

The adoption of this 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 standard

Readers not already familiar with ISO/IEC 27002 are urged to read the introductory sections of that standard before continuing. Implementers of the present standard (27799) must first thoroughly read ISO/IEC 27002, as the text below will frequently refer the reader to the relevant sections of that standard. The present document cannot be fully understood without access to the full text of ISO/IEC 27002.

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

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

Once the 27002 standard has been put into place, effective ongoing management is considered essential if the benefits of the standard are to be maintained. Section 0 discusses compliance assessment and the requirements for ongoing information security management.

This standard concludes with four informative appendices. The first describes the general threats to health information. The second briefly describes other standards that can be applied to specific aspects of health information security. The third discusses the advantages of support tools as an aid to implementation. The fourth appendix lists related standards in health information security.

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

1 Scope

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

1.1 General

This standard defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 (Information Technology — Security techniques — Code of practice for information security controls) and is a companion to that standard.[5]

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

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

This 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 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 standard describes.

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

1.2 Scope exclusions

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

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

b) methodologies for pseudonymisation of personal health information (see Annex D for a brief description of an ISO technical specification that deals specifically with this topic);

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

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

[5] This guideline is consistent with the revised version of ISO/IEC 27002:2013.