BS EN ISO 27799:2016

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS EN ISO 27799:2016

National foreword

This British Standard is the UK implementation of EN ISO 27799:2016. It supersedes BS EN ISO 27799:2008 which is withdrawn.

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.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 87253 2

ICS 35.240.80

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 August 2016.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS EN ISO 27799:2016

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO 27799

August 2016

ICS 35.240.80

Supersedes EN ISO 27799:2008

English Version

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

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

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

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

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

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

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

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

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

© 2016 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. EN ISO 27799:2016 E

Documents
Document Sharing Hub

Full document details: BS EN ISO 27799:2016

European foreword

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

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

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

This document supersedes EN ISO 27799:2008.

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

Endorsement notice

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

Documents
Document Sharing Hub

Full document details: BS EN ISO 27799:2016

Contents

Page

Foreword ... **vii**
Introduction ... **viii**
1 Scope ... **1**
2 Normative references ... **2**
3 Terms and definitions ... **2**
4 Structure of this International Standard ... **3**
5 Information security policies ... **4**
5.1 Management direction for information security ... 4
5.1.1 Policies for information security ... 4
5.1.2 Review of the policies for information security ... 5
6 Organization of information security ... **6**
6.1 Internal organization ... 6
6.1.1 Information security roles and responsibilities ... 6
6.1.2 Segregation of duties ... 7
6.1.3 Contact with authorities ... 7
6.1.4 Contact with special interest groups ... 7
6.1.5 Information security in project management ... 8
6.2 Mobile devices and teleworking ... 8
6.2.1 Mobile device policy ... 8
6.2.2 Teleworking ... 9
7 Human resource security ... **9**
7.1 Prior to employment ... 9
7.1.1 Screening ... 9
7.1.2 Terms and conditions of employment ... 10
7.2 During employment ... 11
7.2.1 Management responsibilities ... 11
7.2.2 Information security awareness, education and training ... 11
7.2.3 Disciplinary process ... 11
7.3 Termination and change of employment ... 12
7.3.1 Termination or change of employment responsibilities ... 12
8 Asset management ... **12**
8.1 Responsibility for assets ... 12
8.1.1 Inventory of assets ... 12
8.1.2 Ownership of assets ... 13
8.1.3 Acceptable use of assets ... 13
8.1.4 Return of assets ... 13
8.2 Information classification ... 14
8.2.1 Classification of information ... 14
8.2.2 Labelling of information ... 15
8.2.3 Handling of assets ... 15
8.3 Media handling ... 16
8.3.1 Management of removable media ... 16
8.3.2 Disposal of media ... 16
8.3.3 Physical media transfer ... 17
9 Access control ... **17**
9.1 Business requirements of access control ... 17
9.1.1 Access control policy ... 17
9.1.2 Access to networks and network services ... 18
9.2 User access management ... 18
9.2.1 User registration and de-registration ... 18
9.2.2 User access provisioning ... 19

© ISO 2016 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

9.2.3 Management of privileged access rights 19
9.2.4 Management of secret authentication information of users 20
9.2.5 Review of user access rights 20
9.2.6 Removal or adjustment of access rights 21
9.3 User responsibilities 21
9.3.1 Use of secret authentication information 21
9.4 System and application access control 22
9.4.1 Information access restriction 22
9.4.2 Secure log-on procedures 22
9.4.3 Password management system 22
9.4.4 Use of privileged utility programs 23
9.4.5 Access control to program source code 23

10 Cryptography 23
10.1 Cryptographic controls 23
10.1.1 Policy on the use of cryptographic controls 23
10.1.2 Key management 24

11 Physical and environmental security 24
11.1 Secure areas 24
11.1.1 Physical security perimeter 24
11.1.2 Physical entry controls 25
11.1.3 Securing offices, rooms and facilities 25
11.1.4 Protecting against external and environmental threats 25
11.1.5 Working in secure areas 25
11.1.6 Delivery and loading areas 25
11.2 Equipment 26
11.2.1 Equipment siting and protection 26
11.2.2 Supporting utilities 26
11.2.3 Cabling security 27
11.2.4 Equipment maintenance 27
11.2.5 Removal of assets 27
11.2.6 Security of equipment and assets off-premises 27
11.2.7 Secure disposal or reuse of equipment 28
11.2.8 Unattended user equipment 28
11.2.9 Clear desk and clear screen policy 28

12 Operations security 29
12.1 Operational procedures and responsibilities 29
12.1.1 Documented operating procedures 29
12.1.2 Change management 29
12.1.3 Capacity management 30
12.1.4 Separation of development, testing and operational environments 30
12.2 Protection from malware 30
12.2.1 Controls against malware 30
12.3 Backup 31
12.3.1 Information backup 31
12.4 Logging and monitoring 31
12.4.1 Event logging 31
12.4.2 Protection of log information 32
12.4.3 Administrator and operator logs 33
12.4.4 Clock synchronisation 34
12.5 Control of operational software 34
12.5.1 Installation of software on operational systems 34
12.6 Technical vulnerability management 34
12.6.1 Management of technical vulnerabilities 34
12.6.2 Restrictions on software installation 35
12.7 Information systems audit considerations 35
12.7.1 Information systems audit controls 35

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

13 Communications security ... **35**
13.1 Network security management ... 35
13.1.1 Network controls ... 35
13.1.2 Security of network services ... 36
13.1.3 Segregation in networks ... 36
13.2 Information transfer ... 36
13.2.1 Information transfer policies and procedures ... 36
13.2.2 Agreements on information transfer ... 37
13.2.3 Electronic messaging ... 37
13.2.4 Confidentiality or non-disclosure agreements ... 38

14 System acquisition, development and maintenance ... **38**
14.1 Security requirements of information systems ... 38
14.1.1 Information security requirements analysis and specification ... 38
14.1.2 Securing application services on public networks ... 40
14.1.3 Protecting application services transactions ... 40
14.2 Security in development and support processes ... 40
14.2.1 Secure development policy ... 40
14.2.2 System change control procedures ... 41
14.2.3 Technical review of applications after operating platform changes ... 41
14.2.4 Restrictions on changes to software packages ... 41
14.2.5 Secure system engineering principles ... 42
14.2.6 Secure development environment ... 42
14.2.7 Outsourced development ... 42
14.2.8 System security testing ... 42
14.2.9 System acceptance testing ... 43
14.3 Test data ... 43
14.3.1 Protection of test data ... 43

15 Supplier relationships ... **43**
15.1 Information security in supplier relationships ... 43
15.1.1 Information security policy for supplier relationships ... 43
15.1.2 Addressing security within supplier agreements ... 44
15.1.3 Information and communication technology supply chain ... 44
15.2 Supplier service delivery management ... 44
15.2.1 Monitoring and review of supplier services ... 45
15.2.2 Managing changes to supplier services ... 45

16 Information security incident management ... **45**
16.1 Management of information security incidents and improvements ... 45
16.1.1 Responsibilities and procedures ... 45
16.1.2 Reporting information security events ... 45
16.1.3 Reporting information security weaknesses ... 46
16.1.4 Assessment of and decision on information security events ... 47
16.1.5 Response to information security incidents ... 47
16.1.6 Learning from information security incidents ... 47
16.1.7 Collection of evidence ... 47

17 Information security aspects of business continuity management ... **48**
17.1 Information security continuity ... 48
17.1.1 Planning information security continuity ... 48
17.1.2 Implementing information security continuity ... 49
17.1.3 Verify, review and evaluate information security continuity ... 49
17.2 Redundancies ... 49
17.2.1 Availability of information processing facilities ... 49

18 Compliance ... **50**
18.1 Compliance with legal and contractual requirements ... 50
18.1.1 Identification of applicable legislation and contractual requirements ... 50
18.1.2 Intellectual property rights ... 50
18.1.3 Protection of records ... 50

AVA Documents
Document Sharing Hub

© ISO 2016 – All rights reserved

Full document details: BS EN ISO 27799:2016

18.1.4 Privacy and protection of personally identifiable information ... 51
18.1.5 Regulation of cryptographic controls ... 52
18.2 Information security reviews ... 52
18.2.1 Independent review of information security ... 52
18.2.2 Compliance with security policies and standards ... 52
18.2.3 Technical compliance review ... 53

Annex A (informative) **Threats to health information security** ... **54**

Annex B (informative) **Practical action plan for implementing ISO/IEC 27002 in healthcare** ... **59**

Annex C (informative) **Checklist for conformance to ISO 27799** ... **72**

Bibliography ... **98**

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS EN ISO 27799:2016

Foreword

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

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

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

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

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

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

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

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

Introduction

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

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

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

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

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

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

Objectives

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

© ISO 2016 – All rights reserved
AVA Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

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

Health information to be protected

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

a) personal health information,

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

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

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

e) data on health professionals, staff and volunteers,

f) information related to public health surveillance,

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

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

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

Threats and vulnerabilities in health information security

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

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

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

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

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

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

Who should read this International Standard?

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

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

Benefits of using this International Standard

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

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

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

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

How to use this International Standard

Documents
Document Sharing Hub

© ISO 2016 – All rights reserved

Full document details: BS EN ISO 27799:2016

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

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

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

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

This International Standard concludes with four informative appendices.

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

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

1 Scope

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

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

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

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

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

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

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

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

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

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

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

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

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS EN ISO 27799:2016

2 Normative references

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

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

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

3 Terms and definitions

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

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

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

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

[SOURCE: ISO/TR 20514:2005]

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

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

3.4
healthcare organization
organization that provides healthcare services

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

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

[SOURCE: ISO 17090-1:2013]

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

[SOURCE: ISO 22857:2013, 3.7]

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

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

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

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

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

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

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

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

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

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

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

[SOURCE: ISO 18308:2011, 3.47]

4 Structure of this International Standard

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

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

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

<u>Health-specific control</u>

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

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

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

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

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

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

5 Information security policies

5.1 Management direction for information security

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

5.1.1 Policies for information security

Control

ISO/IEC 27002:2013, 5.1.1, applies.

Health-specific control

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

Implementation guidance

ISO/IEC 27002:2013, 5.1.1, applies.

Health-specific implementation guidance

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

a) the need for health information security;

b) the goals of health information security;

c) compliance scope, as described in Clause 18;

d) legislative, regulatory, and contractual requirements, including those for the protection of personal health information and the legal and ethical responsibilities of health professionals to protect this information;

e) arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentiality, without fear of blame or recrimination;

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

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

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

a) the breadth of health information;

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

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

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

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

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

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

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

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

j) the implications of security measures on patient safety;

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

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

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

Other information

ISO/IEC 27002:2013, 5.1.1, applies.

5.1.2 Review of the policies for information security

Control

ISO/IEC 27002:2013, 5.1.2, applies.

Health-specific control

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

Implementation guidance

ISO/IEC 27002:2013, 5.1.2, applies.

Health-specific implementation guidance

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

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

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

c) the changes identified in the external environment that similarly impact the organization's risk profile;

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

d) the latest controls, compliance and assurance requirements and arrangements mandated by jurisdictional health bodies or by new legislation or regulation;

e) the latest guidance and recommendations from health professional associations and from information privacy commissioners regarding the protection of personal health information;

f) the results of legal cases tested in the courts, which have established or negated precedents or established practices;

g) the challenges and issues regarding the policy, as expressed to the organization by its staff, subjects of care and their partners and care givers, researchers and governments (e.g. privacy commissioners);

h) reports on patient safety incidents in order to devise mitigations in those cases where the patient safety incident is the result of failures of information security measures.

6 Organization of information security

6.1 Internal organization

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

6.1.1 Information security roles and responsibilities

Control

ISO/IEC 27002:2013, 6.1.1, applies.

Health-specific control

Organizations processing personal health information shall:

a) clearly define and assign information security responsibilities;

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

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

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

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

Implementation guidance

ISO/IEC 27002:2013, 6.1.1, applies.

Health-specific implementation guidance

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

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

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

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

Other information

ISO/IEC 27002:2013, 6.1.1, applies.

6.1.2 Segregation of duties

Control

ISO/IEC 27002:2013, 6.1.2, applies.

Health-specific control

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

Implementation guidance

ISO/IEC 27002:2013, 6.1.2, applies.

Other information

ISO/IEC 27002:2013, 6.1.2, applies.

6.1.3 Contact with authorities

Control

ISO/IEC 27002:2013, 6.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 6.1.3, applies.

6.1.4 Contact with special interest groups

Control

ISO/IEC 27002:2013, 6.1.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.1.4, applies.

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 6.1.4, applies.

6.1.5 Information security in project management

Control

ISO/IEC 27002:2013, 6.1.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.1.5, applies.

Health-specific control

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

Health-specific implementation guidance

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

Other health-specific information.

ISO/IEC 27002:2013, 6.1, applies.

6.2 Mobile devices and teleworking

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

6.2.1 Mobile device policy

Control

ISO/IEC 27002:2013, 6.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.2.1, applies.

Health-specific implementation guidance

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

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

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

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

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

© ISO 2016 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

Other information

ISO/IEC 27002:2013, 6.2.1, applies.

6.2.2 Teleworking

Control

ISO/IEC 27002:2013, 6.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 6.2.2, applies.

Health-specific implementation guidance

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

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

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

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

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

Other information

ISO/IEC 27002:2013, 6.2.2, applies.

7 Human resource security

7.1 Prior to employment

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

7.1.1 Screening

Control

ISO/IEC 27002:2013, 7.1.1, applies.

Health-specific controls

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

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

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

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

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

Implementation guidance

ISO/IEC 27002:2013, 7.1.1, applies.

Health-specific implementation guidance

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

7.1.2 Terms and conditions of employment

Control

ISO/IEC 27002:2013, 7.1.2, applies.

Health-specific control

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

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

Implementation guidance

ISO/IEC 27002:2013, 7.1.2, applies.

Health-specific implementation guidance

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

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

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

Other information

ISO/IEC 27002:2013, 7.1.2, applies.

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

7.2 During employment

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

7.2.1 Management responsibilities

Control

ISO/IEC 27002:2013, 7.2.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 7.2.1, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note the special emphasis that needs to be placed on the concerns of subjects of care who do not wish their personal health information to be accessed by health workers who are neighbours, colleagues, or relatives. Such concerns often make up a large percentage of complaints from those with fears about the confidentiality of their personal health information. Likewise, staff members often do not wish to be placed unnecessarily in the position of reviewing information about friends, relatives, or neighbours. Effective management of health information systems needs to address these concerns.

Other information

ISO/IEC 27002:2013, 7.2.1, applies.

7.2.2 Information security awareness, education and training

Control

ISO/IEC 27002:2013, 7.2.2, applies.

Health-specific control

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

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

Implementation guidance

ISO/IEC 27002:2013, 7.2.2, applies.

Other information

ISO/IEC 27002:2013, 7.2.2, applies.

7.2.3 Disciplinary process

Control

ISO/IEC 27002:2013, 7.2.3, applies.

Implementation guidance

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

ISO/IEC 27002:2013, 7.2.3, applies.

Health-specific implementation guidance

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

Other information

ISO/IEC 27002:2013, 7.2.3, applies.

7.3 Termination and change of employment

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

7.3.1 Termination or change of employment responsibilities

Control

ISO/IEC 27002:2013, 7.3.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 7.3.1, applies.

Health-specific implementation guidance

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

Other information

ISO/IEC 27002:2013, 7.3.1, applies.

8 Asset management

8.1 Responsibility for assets

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

8.1.1 Inventory of assets

Control

ISO/IEC 27002:2013, 8.1.1, applies.

Health-specific control

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

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

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

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

Implementation guidance

ISO/IEC 27002:2013, 7.3.1, applies.

Health-specific implementation guidance

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

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

Other information

ISO/IEC 27002:2013, 7.3.1, applies.

8.1.2 Ownership of assets

Control

ISO/IEC 27002:2013, 8.1.2, applies.

Assets maintained in the inventory should be owned.

Implementation guidance

ISO/IEC 27002:2013, 8.1.2, applies.

Health-specific implementation guidance

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

Other information

ISO/IEC 27002:2013, 8.1.2, applies.

8.1.3 Acceptable use of assets

Control

ISO/IEC 27002:2013, 8.1.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 8.1.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

8.1.4 Return of assets

Control

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

ISO/IEC 27002:2013, 8.1.4, applies.

Health-specific control

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

Implementation guidance

ISO/IEC 27002:2013, 8.1.4, applies.

8.2 Information classification

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

8.2.1 Classification of information

Control

ISO/IEC 27002:2013, 8.2.1, applies.

Health-specific control

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

Implementation guidance

ISO/IEC 27002:2013, 8.2.1, applies.

Health-specific implementation guidance

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

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

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

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

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

© ISO 2016 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

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

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

Other information

ISO/IEC 27002:2013, 8.2.1, applies.

8.2.2 Labelling of information

Control

ISO/IEC 27002:2013, 8.2.2, applies.

Health-specific control

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

Implementation guidance

ISO/IEC 27002:2013, 8.2.2, applies.

Health-specific implementation guidance

Not all health information is confidential and not all health information systems provide users with access to personal health information. Users of health information systems need to know when the data they are accessing contains personal health information.

Other information

ISO/IEC 27002:2013, 8.2.2, applies.

8.2.3 Handling of assets

Control

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

ISO/IEC 27002:2013, 8.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 8.2.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

8.3 Media handling

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

8.3.1 Management of removable media

Control

ISO/IEC 27002:2013, 8.3.1, applies.

Health-specific control

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

Implementation guidance

ISO/IEC 27002:2013, 8.3.1, applies.

Health-specific implementation guidance

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

a) encrypted while its media are in transit, or

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

8.3.2 Disposal of media

Control

ISO/IEC 27002:2013, 8.3.2, applies.

Health-specific control

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

Implementation guidance

ISO/IEC 27002:2013, 8.3.2, applies.

Health-specific implementation guidance

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

Other information

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

ISO/IEC 27002:2013, 8.3.21, applies.

8.3.3 Physical media transfer

Control

ISO/IEC 27002:2013, 8.3.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 8.3.3, applies.

Health-specific implementation guidance

No additional guidance for information security management in health.

Other information

ISO/IEC 27002:2013, 8.3.3, applies.

9 Access control

9.1 Business requirements of access control

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

9.1.1 Access control policy

Control

ISO/IEC 27002:2013, 9.1.1, applies.

Health-specific control

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

a) when a healthcare relationship exists between the user and the data subject (the subject of care whose personal health information is being accessed);

b) when the user is carrying out an activity on behalf of the data subject;

c) when there is a need for specific data to support this activity.

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

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

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

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

Implementation guidance

ISO/IEC 27002:2013, 9.1.1, applies.

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

Health-specific implementation guidance

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

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

Other information

ISO/IEC 27002:2013, 9.1.1, applies.

Other health-specific information

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

9.1.2 Access to networks and network services

Control

ISO/IEC 27002:2013, 9.1.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.1.2, applies.

Other information

ISO/IEC 27002:2013, 9.1.2, applies.

9.2 User access management

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

9.2.1 User registration and de-registration

Control

ISO/IEC 27002:2013, 9.2.1, applies.

Health-specific control

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

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

Implementation guidance

ISO/IEC 27002:2013, 9.2.1, applies.

Health-specific implementation guidance

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

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

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

c) the assignment of an unambiguous user identifier.

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

Other information

ISO/IEC 27002:2013, 9.2.1, applies.

9.2.2 User access provisioning

Control

ISO/IEC 27002:2013, 9.2.2, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.2.2, applies.

Health-specific implementation guidance

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

Other information

ISO/IEC 27002:2013, 9.2.2, applies.

9.2.3 Management of privileged access rights

Control

ISO/IEC 27002:2013, 9.2.3, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.2.3, applies.

Health-specific implementation guidance

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

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

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

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

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

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

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

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

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

Other information

ISO/IEC 27002:2013, 9.2.3, applies.

9.2.4 Management of secret authentication information of users

Control

ISO/IEC 27002:2013, 9.2.4, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.2.4, applies.

Health-specific implementation guidance

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.

Other information

ISO/IEC 27002:2013, 9.2.4, applies.

9.2.5 Review of user access rights

Control

ISO/IEC 27002:2013, 9.2.5, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.2.5, applies.

Health-specific 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.

Other information

© ISO 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016

ISO/IEC 27002:2013, 9.2.5, applies.

9.2.6 Removal or adjustment of access rights

Control

ISO/IEC 27002:2013, 9.2.6, applies.

Health-specific control

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

Implementation guidance

ISO/IEC 27002:2013, 9.2.6, applies.

Health-specific implementation guidance

In addition to the guidance given by ISO/IEC 27002, it is important to note the many examples in healthcare of students, interns and locums who have retained their access privileges after cessation of their internship, locum, etc. Especially in large hospitals, large numbers of temporary staff will typically have short-term access to personal health information. The termination of the access rights of such staff needs to be carefully managed. At the same time, in healthcare, many transactions take place well after the time of care (e.g. the sign-off of medical transcriptions). This can significantly complicate the process of removing access rights in a timely fashion and these transactions should be taken into account when designing and implementing procedures on the removal of access rights.

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

Other information

ISO/IEC 27002:2013, 9.2.6, applies.

9.3 User responsibilities

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

9.3.1 Use of secret authentication information

Control

ISO/IEC 27002:2013, 9.3.1, applies.

Implementation guidance

ISO/IEC 27002:2013, 9.3.1, applies.

Health-specific implementation guidance

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

Other information

ISO/IEC 27002:2013, 9.3.1, applies.

© ISO 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS EN ISO 27799:2016