AS ISO 27799—2011

Australian Standard®

Information security management in health using ISO/IEC 27002

This Australian Standard® was prepared by Committee IT-014, Health Informatics. It was approved on behalf of the Council of Standards Australia on 8 March 2011.
This Standard was published on 21 April 2011.

The following are represented on Committee IT-014:

- Aged Care Association Australia
- Australasian College of Health Informatics
- Australian and New Zealand College of Anaesthetists
- Australian Healthcare and Hospitals Association
- Australian Institute of Health & Welfare
- Australian Institute of Radiography
- Australian Private Hospitals Association
- Central Queensland University
- Commonwealth Department of Health and Ageing
- Consumers Federation of Australia
- Consumers' Health Forum of Australia
- CSIRO e-Health Research Centre
- Department of Health Western Australia
- Department of Human Services (Victoria)
- Engineers Australia
- Health Information Management Association of Australia
- HL7 Australia
- Medical Software Industry Association
- Medicare Australia
- National E Health Transition Authority
- NSW Health Department
- Queensland Health
- Royal Australian College of General Practitioners
- Royal Australian College of Medical Administrators
- Royal College of Nursing, Australia
- Royal College of Pathologists of Australasia
- The Royal Australian and New Zealand College of Radiologists
- University of Western Sydney

The following are represented on Subcommittee IT-014-04:

- Anson Consulting
- Attorney-General's Department
- Central Queensland University
- Commonwealth Department of Health and Ageing
- Data Systematics
- DH4
- eClinic
- Edith Cowan University
- Emerging Systems
- ISN Solutions
- Lockstep Consulting
- Michael Legg & Associates
- National E-Health Transition Authority
- Professional Management Solutions
- Queensland Health
- Queensland University of Technology
- Royal Prince Alfred Hospital
- SeeBeyond
- The Pharmacy Guild of Australia
- University of Tasmania

This Standard was issued in draft form for comment as DR AS ISO/IEC 5223.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting **www.standards.org.au**

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at **mail@standards.org.au**, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard®

Information security management in health using ISO/IEC 27002

First published as AS ISO 27799—2011.

Published by SAI Global Limited under licence from Standards Australia Limited, GPO Box 476, Sydney, NSW 2001, Australia

ISBN 978 0 7337 9836 8

PREFACE

This Standard was prepared by the Standards Australia Committee IT-014, Health Informatics and Subcommittee, IT-014-04, Information Security.

The objective of this Standard is to specify guidance on healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information by implementing ISO/IEC 27002 which has been adopted by Standards Australia and Standards New Zealand as AS/NZS ISO/IEC 27002.

This Standard is identical with, and has been reproduced from ISO 27799:2008, *Health informatics — Information security management in health using ISO/IEC 27002*.

As this Standard is reproduced from an International Standard, the following applies:

(a) Its number appears on the cover and title page while the International Standard number appears only on the cover.

(b) In the source text 'this International Standard' should read 'this Australian Standard'.

(c) A full point substitutes for a comma when referring to a decimal marker.

(d) In Clause 6.4.4.3 *add* the following paragraph:

Maintaining privacy of subjects of care depends upon maintaining the confidentiality of personal health information. Security risk assessments can address many concerns regarding the confidentiality of health information; however, a privacy impact assessment (PIA) is also required in respect of the applicable laws, regulations and any contractual arrangements that apply.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard	*Australian Standard*
ISO/IEC 27002 Information technology—Security techniques—Code of practice for information security management	AS/NZS ISO/IEC 27002 Information technology—Security techniques—Code of practice for information security management

Funding for this publication has been provided by the Commonwealth Department of Health and Ageing. The Commonwealth makes no representation or warranty that the information in this publication is correct and accurate.

Standards Australia wishes to thank the Department of Health and Ageing for their continued financial support in helping us develop this Australian Standard.

CONTENTS

Page

INTRODUCTION

This International Standard provides guidance to healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information by implementing ISO/IEC 27002[1)]. Specifically, this International Standard addresses the special information security management needs of the health sector and its unique operating environments. While the protection and security of personal information is important to all individuals, corporations, institutions and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, auditability and availability of personal health information. This type of information is regarded by many as being among the most confidential of all types of personal information. Protecting this confidentiality is essential if the privacy of subjects of care is to be maintained. The integrity of health information must be protected to ensure patient safety, and an important component of that protection is ensuring that the information's entire life cycle be fully auditable. The availability of health information is also critical to effective healthcare delivery. Health informatics systems must meet unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks. Protecting the confidentiality, integrity and availability of health information therefore requires health-sector-specific expertise.

The need for effective IT security management in healthcare is made all the more urgent by the increasing use of wireless and Internet technologies in healthcare delivery. If not implemented properly, these complex technologies will increase the risks to the confidentiality, integrity and availability of health information. Regardless of size, location and model of service delivery, all healthcare organizations need to have stringent controls in place to protect the health information entrusted to them. Yet many health professionals work as solo health providers or in small clinics that lack the dedicated IT resources to manage information security. Healthcare organizations must therefore have clear, concise and healthcare-specific guidance on the selection and implementation of such controls. This guidance must be applicable to the wide range of sizes, locations, and models of service delivery found in healthcare. Finally, with increasing electronic exchange of personal health information between health professionals, there is a clear benefit in adopting a common reference for information security management in healthcare.

ISO/IEC 27002 is already being used extensively for health informatics IT security management through the agency of national or regional guidelines in Australia, Canada, France, the Netherlands, New Zealand, South Africa and the United Kingdom. Interest is growing in other countries as well. This International Standard (ISO 27799) draws upon the experience gained in these national endeavours in dealing with the security of personal health information and is intended as a companion document to ISO/IEC 27002. It is not intended to supplant ISO/IEC 27002 or ISO/IEC 27001. Rather, it is a complement to these more generic standards.

This International Standard applies ISO/IEC 27002 to the healthcare domain in a way that carefully considers the appropriate application of security controls for the purposes of protecting personal health information. These considerations have, in some cases, led the authors to conclude that application of certain ISO/IEC 27002 control objectives is essential if personal health information is to be adequately protected. This International Standard therefore places constraints upon the application of certain security controls specified in ISO/IEC 27002. This in turn has led to the inclusion in Clause 7 of several normative statements stating that the application of a given security control is mandatory. For example, 7.2.1 states that

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

---

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

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

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

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

Who should read this International Standard?

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

Benefits of using this International Standard

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

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

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

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

How to use this International Standard

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

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

Readers seeking guidance on how to implement ISO/IEC 27002 in a health environment will find a practical action plan described in Clause 6. No mandatory requirements are contained in this clause. Instead, general advice and guidance are given on how best to proceed with the implementation of 27002 in healthcare. The clause is organized around a cycle of activities (plan/do/check/act) that are described in ISO/IEC 27001 and that, when followed, will lead to a robust implementation of an information security management system.

Readers seeking specific advice on the eleven security control clauses and 39 main security control categories described in ISO/IEC 27002 will find it in Clause 7. This clause leads the reader through each of the eleven security control clauses of ISO/IEC 27002. Minimum requirements are stated where appropriate and, in some cases, normative guidelines are set out on the proper application of certain ISO/IEC 27002 security controls to the protection of health information.

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

AUSTRALIAN STANDARD

Information security management in health using ISO/IEC 27002

1 Scope

1.1 General

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

This International Standard specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this International Standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information.

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

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

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

1.2 Scope exclusions

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

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

b) methodologies for pseudonymization of personal health information (see bibliographic Reference [10] for an example of an ISO Technical Specification that deals specifically with this subject);

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

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

---

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