This is a free page sample. Access the full version online.

AS ISO 27799—2011
ISO 27799:2008

AS ISO 27799—2011

Australian Standard®

Information security management in health using ISO/IEC 27002

STANDARDS
Australia

This is a free page sample. Access the full version online.

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.

This is a free page sample. Access the full version online.

Australian Standard®

Information security management in health using ISO/IEC 27002

First published as AS ISO 27799—2011.

COPYRIGHT

© Standards Australia Limited

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968.

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

ISBN 978 0 7337 9836 8

This is a free page sample. Access the full version online.

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.

This is a free page sample. Access the full version online.

CONTENTS

Page

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

2 Normative references ... 2

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

4 Abbreviated terms ... 5

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

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

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

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

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

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

Bibliography ... 57

SAI GLOBAL

This is a free preview. Purchase the entire publication at the link below:

Product Page

Looking for additional Standards? Visit Intertek Inform Infostore

Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation