HB 174—2003

Information security management

Implementation guide for the health sector

Standards Australia

This Handbook was prepared by Committee IT-014, Health Informatics. It was published on 10 March 2003.

The following are represented on Committee IT-014:

Australian Association of Pathology Practices Inc
Australian Health Insurance Association
Australian Information Industry Association
Australian Institute of Health and Welfare
Australian Institute of Radiography
Australian Medical Association
Australian Private Hospitals Association
Australian and New Zealand College of Anaesthetists
Central Queensland University
Commonwealth Department of Health and Ageing
Consumers' Federation of Australia
Consumers' Health Forum of Australia
Department of Human Services, South Australia
Department of Human Services, Victoria
General Practice Computing Group
Health Department of Western Australia
Health Information Management Association of Australia
Health Insurance Commission
Health Professions Council of Australia
Institution of Engineers Australia
Medical Industry Association of Australia Inc
Medical Software Industry Association
New South Wales Health Department
National Health Information Management Group
Pharmaceutical Society of Australia
Queensland Health
Royal Australian College of Medical Administrators
Royal College of Nursing, Australia
Royal College of Pathologists of Australia
Society of Hospital Pharmacists of Australia
The Pharmacy Guild of Australia
The Royal Australia and New Zealand College of Radiologists
The University of Sydney

Handbook

Information security management—Implementation guide for the health sector

First published as HB 174—2003.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 4886 4

This page left intentionally blank

Preface

The purpose of these guidelines is to interpret AS/NZS 17799:2001—Information Technology—Code of Practice for Information Security Management, and apply this standard specifically to the interests and unique information security requirements of the Australian Health Sector. **This handbook provides a set of detailed controls, which may be considered best practices in information security.**

These guidelines have been developed by Standards Australia/Standards New Zealand Committee on Health Informatics Privacy & Security (IT-01-04) with assistance from various Australian health sector professionals. This handbook has been developed to address the special considerations that are required for the health sector, with particular emphasis on **individuals and small to medium sized health practitioners.** Overall, the AS/NZS 17799 standard provides an excellent information security management strategy, but as this standard has been designed to encompass a broad range of industries and organisations, and of all sizes, the standard alone cannot be targeted effectively or appropriately to the Health Sector.

The protection and security of information is of prime importance to all individuals, government agencies and firms. For the Health Sector, there is added emphasis on the requirements for confidentiality, privacy, integrity and availability. Naturally, all organisations, regardless of size, must have stringent controls in place for the protection of information. It is therefore critical for an organisation to implement a suitable set of controls and procedures to address information security, and once implemented, the organisation must retain a pre-requisite level of security.

With increasing electronic exchange of patient information between Health Providers, there is a clear benefit in adopting a common reference handbook for information security management.

Not all of the controls described in this Standard will be relevant to every situation. This guide cannot take account of local, environmental and technological constraints, nor can it be presented in a form that is completely applicable to every Health Provider. Health Providers must apply these recommendations to each of their unique circumstances.

In drafting this guide, we have assumed that a health service professional or a member of the supporting administration staff (and not necessarily an information security professional) will most likely undertake the execution of recommendations. For this reason, we have designed this guide such that it appeals to health professionals and non-computing professionals and we have ensured that the guide is clear, concise and easy to understand and interpret. The content is therefore **not** of a highly technical nature.

Our guidelines shall serve two fundamental objectives, specifically:

1. Guidance to ensure that patient privacy is maintained by securing paper and electronic based health records and ensuring the long term integrity and quality of this stored information.
2. Assistance in establishing an appropriate level of health information security for your organisation as a whole.

By following these guidelines, in addition to undertaking an information security management best practice initiative, we aim to greatly assist your health organisation in compliance with the Privacy Amendment (Private Sector) Act 2000*, or your relevant state privacy legislation.

Application

This handbook has been written for health professionals seeking to conform to the information security management specifications of the AS/NZS 17799 standard. Whilst these guidelines are specifically focussed on individuals and small to medium sized health organisations, larger businesses and government departments, who may have specialised information security or privacy personnel, will also find these guidelines of significant use and benefit.

Our intended audience may include, but is not limited to:

- Health Consumers
- Health Service Providers
- Medical Centres
- Public and Private Hospitals
- Pharmacies
- Information Repositories
- Clinical Registries
- Health Funders
- Health Agencies

A glossary covering Computing, Security and Privacy terms and definitions has been included. We recommend that all readers of the handbook make themselves familiar with our definitions.

* More information about the Act can be obtained from the Federal Privacy Commission website. www.privacy.gov.au. You will find specific information about how the Privacy Act may affect your health business.

For the purposes of this guide and in the context of the health sector, the Australian Bureau of Statistics has provided the following definitions covering small and medium businesses:

- A ***Small*** business—This may range from small groups of people through to businesses that operate with up to 20 staff members. Examples include pharmacies and general medical practices.

- A ***Medium*** business—Those businesses with staff members of approximately 20-199 people. Examples include small private hospitals, medical facilities, and pathology practices.

Contents

Introduction

What is Health Information Security?

Health Information is an important asset for Health Providers, and this asset needs to be adequately protected. The primary focus of Health Information Security relates to the protection and safeguarding of patient information and the requirement to protect the privacy of patients. In addition, Health Providers must ensure that information is accurate and available whenever required.

Information may exist in many forms. From the perspective of the Health Sector, information is not necessarily only words and numbers, but this may also extend to photographs, drawings, video footage, slides, and x-rays. Information can be printed or written, stored electronically, transmitted by post or using electronic means, shown on film or spoken as part of normal conversation. Whatever form the information takes, or means by which it is shared or stored, the information should always be appropriately protected.

In essence, the protection of information involves the preservation of the following:

- ***Confidentiality***—information should only be accessible and available to those authorised to have access.
- ***Integrity***—information should be stored, used, transferred and retrieved in manners such that there is confidence that the information has not been tampered with or modified other than as authorised.
- ***Availability***—ensures that information is accessible to authorised individuals when and where required.

It is important to note that there are differences between ***privacy*** and ***confidentiality***. Privacy is concerned with information handling processes of personal and sensitive information. Privacy deals with ensuring that this information is not disclosed for any purpose other than for which it was collected, without appropriate consent.

How do I secure my health information?

Information security is achieved by implementing a suitable set of controls. A control may constitute a policy, a practice, a set of procedures, or perhaps a software function. These controls need to be established in order to ensure that the specific security objectives of the organisation are met. Although at first this may appear daunting, this handbook will help you to understand ***what*** controls are available and ***how*** they may be implemented. By reading this handbook you will be in a position to better ***understand the information that you are protecting*** and then you will be able to select those controls appropriate for providing protection in your unique health environment.