

INFORMATION SHEET 8 – SECURITY OF INFORMATION

Quick Reference

This information is primarily intended for Administrative Staff and Health Practitioners

Definition of 'health information' is specified in Part 1, Section 3 of the HRA

Undertake a risk management assessment of all information management security measures

INTRODUCTION

Privacy Law requires that personal and health information (Health Privacy Principle 4 and Information Privacy Principle 4) be protected from misuse and loss and from unauthorised access, modification or disclosure. Essentially this relates to the provision of security, retention and disposal of information. This Information Sheet deals with security issues only. Retention and disposal of data are dealt with in Information Sheet 9.

WHAT IS HEALTH INFORMATION?

Health information is broadly defined in the Health Records Act 2001 (HRA) to include personal information (including an opinion) about a person's physical, mental or psychological health or disability (refer to HRA for complete text).

This would also include, for example x-rays, tissue samples, photographs, video recordings and genetic information.

DOES THE SECURITY PRINCIPLE APPLY TO ALL FORMS OF HEALTH INFORMATION?

All health information must be safeguarded from loss, unauthorised destruction, modification, disclosure or other misuse regardless of whether it is paper based, electronic or in some other form.

To maximise compliance with the security privacy principle, Primary Care Partnership (PCP) member agencies should undertake a risk management assessment of existing electronic and physical security measures to determine if additional safeguards are required. All staff (including volunteers and any contracted service providers) should be made clearly aware of their responsibilities in maintaining the security and confidentiality of consumers' health information.

PHYSICAL SECURITY

Steps that may be taken to secure the physical environment in which personal health information is stored include:

- Access control measures for file storage areas and offices
- Locked filing cabinets and other information storage facilities
- File management tracking system to monitor case file movements
- Adherence to a clean desk policy
- Positioning of fax machines receiving personal health information so that information cannot be viewed from public areas
- Positioning of computer terminals so that information cannot be seen or accessed by unauthorised staff
- Provision of security alarm systems.

INFORMATION SHEET 8 – SECURITY OF INFORMATION

Quick Reference

AS/NZS 7799.2:2000 – The Australian / New Zealand Standard for Information Security Management details a comprehensive set of security controls that form best practice for security protection

Develop guidelines that allow for differing information access levels for administrative personnel and health practitioners

LOGICAL (INFORMATION TECHNOLOGY) SECURITY

The rising use of information technology to support business practices means that an increasing amount of information is transferred and processed by electronic means.

PCP member agencies need to develop security measures that minimise the risk of any misuse of personal health data held in electronic systems. Some strategies that can be put into place include:

- Access control arrangements, including user passwords, lockable screen savers and firewalls to protect information held on networked systems
- Dedicated lines for remote access (eg, where out-posted services are provided)
- e-mail encryption to protect data being transferred between health care providers
- Audit trails included in any database systems used and/or shared between providers
- Disclaimers and appropriate headers / footers / watermarks on documents

PROCEDURAL / ADMINISTRATIVE SECURITY

Health information is highly sensitive and only that information that is directly necessary to enable health practitioners and personnel to carry out their specific functions should be accessed for use. For example:

- Administrators dealing with financial information should not see a consumer's clinical notes
- Ancillary staff such as couriers or office cleaners should not have access to clinical or financial information
- Clinical staff may not normally need to see a consumer's complete medical record, eg, in a community health service consumer health information may be contained in a single record for ease of administration leading to a risk of information being inadvertently disclosed between practitioners

PCP Partnerships should develop clear guidelines for the management of health information that provide unambiguous advice to member agencies and health practitioners on their responsibilities when handling personal health information.

SOME STRATEGIES FOR DEALING WITH INFORMATION SECURITY IN THE NEW PRIVACY ENVIRONMENT

- ❑ Develop and document a range of security measures for inclusion in the Partnership's privacy protocols
- ❑ Provide guidelines and appropriate training for personnel in the handling of health information
- ❑ Ensure that any contracted service providers and fee-for-service professionals are contractually bound to adhere to the organisation's privacy protocols
- ❑ Partnerships must have protocols / agreements with other health care providers around security of information that is shared between health care providers

LEGAL ADVICE: DISCLAIMER

Information contained within this information sheet is not intended to substitute for legal advice. Primary Care Partnerships and / or member agencies should take advice from their legal advisors in determining whether their policies and practices comply with all relevant legislation.