Health Information

and the

Privacy Act 1988

A short guide for the private health sector

www.privacy.gov.au

December 2001

This Guide provides a brief introduction to the Commonwealth privacy law covering the private health sector. For private sector health service providers, the amended Privacy Act 1988 takes effect from 21 December 2001. This Guide does not describe the law in detail.

ISBN 1-877079-37-5

Privacy and Health Care

Access to quality health care is an important priority for all Australians.

It is also important that individuals' privacy is respected during the provision of health care and treatment services. Being reassured about privacy gives consumers the confidence to access the health services they need.

People have different views about their privacy, including when and why it is important. Their views may depend on the sensitivity of the information or their circumstances and beliefs.

At times, health service providers need to share information with each other to ensure that a person receives good quality health care. The *Privacy Amendment (Private Sector) Act 2000*, which amends the *Privacy Act 1988*, allows the sharing of information with others, where necessary, while outlining the privacy issues and safeguards to consider in these circumstances.

Importantly, the legislation gives a person choice about how their health information is handled.

Open communication between health service providers and health consumers regarding the handling of health information is central to properly addressing privacy issues.

Protecting Health Information

In today's health environment, the privacy protection of health information is important for both electronic health records and paper-based records.

When deciding how best to protect a person's health information, health service providers may need to consider:

- Who should be allowed to see hospital medical records, records kept in a pharmacy, or computerised records in a medical practice?
- When and how is it appropriate for one health service to transfer information to another?
- What safeguards must apply when information is used for health research?
- Is the person's consent needed for handling health information in each situation?

This is where the privacy legislation can help.

<< Good privacy - good health care>>

The *Privacy Amendment (Private Sector) Act 2000*

The *Privacy Amendment (Private Sector) Act 2000* amends the Commonwealth *Privacy Act 1988* ('the Privacy Act') to establish minimum privacy standards for the Australian private sector, including for all private sector

organisations that both provide health services and hold health information. The legislation applies from 21 December 2001.

The Privacy Act creates a single, nationally consistent framework for protecting privacy. It complements existing codes of practice and ethics in the health sector.

The Commonwealth legislation prevails over State or Territory privacy legislation, to the extent that these laws are inconsistent.

What is a 'health service'?

The Privacy Act stipulates providing a 'health service' includes any activity that involves:

- assessing, recording, maintaining or improving a person's health; or
- diagnosing or treating a person's illness or disability; or
- dispensing a prescription drug or medicinal preparation by a pharmacist.

The Privacy Act applies to *all* private sector organisations that deliver these types of services, including all small health services that hold health information.

The types of health services covered include traditional health service providers such as private hospitals and day surgeries, medical practitioners, pharmacists, and allied health professionals, as well as complementary

therapists, gyms, weight loss clinics and many others.

<< All private sector health service providers that hold health information are covered>>

What type of information is protected?

The Privacy Act protects 'personal information' about individuals - that is, any information recorded about a person where their identity is known or could reasonably be worked out.

Personal information includes a person's name, address, Medicare number and any health information (including opinion) about the person. Sometimes, details about a person's medical history or other contextual information can identify them, even if no name is attached to the record. This is still 'personal information'.

The Privacy Act does not cover de-identified statistical data, where individuals cannot reasonably be re-identified.

'Health information' is a particular kind of 'personal information' and attracts additional privacy protection because of its greater sensitivity.

'Health information' includes information about a person's health, disability, use of health services, or other personal information collected from someone when delivering a health service.

The National Privacy Principles (NPPs)

Ten NPPs form the core of the private sector provisions of the Privacy Act. These principles set the minimum standards for privacy that organisations must meet.

The principles cover the whole information handling lifecycle – from the collection of health information, to its storage and maintenance, as well as its use and disclosure.

The principles, as they might apply in the health sector, are summarised below. For more details see the Federal Privacy Commissioner's *Guidelines on Privacy in the Private Health Sector.*

NPP 1 – Collection and NPP 10 – Sensitive Information

These principles apply to the collection of health information. In general, they require a health service provider to:

- collect only the information necessary to deliver the health service;
- collect lawfully, fairly and not intrusively; and
- obtain a person's consent to collect health information about them.

Providers also need to ensure that consumers are informed about why their health information is being collected, who is collecting it, how it will be used, to whom it may be given and that they can access it if they wish.

<< Health service providers can collect health information only with consent>>

NPP 2 – Use and Disclosure

This principle sets out how providers can use and disclose health information.

'Use' refers to the handling of information *within* an organisation.

'Disclosure' is the transfer of information to a third party *outside* the organisation.

A health service provider may use or disclose health information:

- for the main reason it was collected (the primary purpose); or
- for directly-related secondary purposes, if the consumer would reasonably expect these; or
- if the consumer gives consent to the proposed use or disclosure; or
- if one of the other provisions under this principle applies.

The key is to make sure that there is alignment between the expectations of the health service provider and those of the consumer about what will be done with the health information.

<< Promote a common understanding about privacy of health information >>

NPP 3 – Data Quality

Health service providers are required to take reasonable steps to keep health information up-to-date, accurate and complete.

<< Health service providers should maintain data quality and integrity >>

NPP 4 – Data Security

This principle requires that health service providers take reasonable steps to protect and secure health information from loss, misuse and unauthorised access. Information that is no longer needed should be destroyed.

As health information may be needed for future care of the individual or for public health reasons, the priority should be to secure the data properly.

<< Health service providers should protect information against security risks >>

NPP 5 – Openness

Health service providers need to be open about how they handle health information.

A provider must develop a document for consumers which clearly explains how their organisation handles health information. The document must be made available to anyone who asks for it.

<< Fewer surprises about handling health information leads to fewer privacy complaints >>

NPP 6 – Access & Correction

Consumers have a general right of access to their own health records.

Access can only be denied in certain circumstances - for instance where access can pose a serious risk to a person's life or health.

Also, consumers can ask for information about them to be corrected, if it is inaccurate, incomplete or out-of-date. The provider will need to take reasonable steps to correct the information.

<< Consumers have a general right of access to their own health records>>

NPP 7 – Identifiers

There are restrictions on how Commonwealth government identifiers, such as the Medicare number or the Veterans Affairs number, can be adopted, used or disclosed.

At present, a health service provider is not permitted to adopt these identifiers for their own record keeping systems. These identifiers may only be used or disclosed for the reasons they were issued or if other provisions under this principle apply.

NPP 8 – Anonymity

Where lawful and practicable, consumers must be given the option to use health services without identifying themselves.

NPP 9 – Transborder data flows

If health information needs to be transferred out of Australia, this may occur if laws (or a scheme) with similar privacy protection to these principles bind the recipient.

Otherwise, health information should only be transferred with the consumer's consent, or if other provisions under this principle apply.

Complaints

Complaints about alleged breaches of privacy can be made to the Federal Privacy Commissioner. The Commissioner can investigate, conciliate and, if necessary, make determinations about complaints. However, the Commissioner will not investigate, unless the complainant has first complained formally to the health service provider concerned.

Guidelines on Privacy in the Private Health Sector

For more assistance on how the privacy legislation applies to health service providers, see the Federal Privacy Commissioner's *Guidelines on Privacy in the Private Health*

Sector and Information Sheets (especially Information Sheet 9-2001 *Handling Health Information for Research and Management*).

These Guidelines and the *Privacy Act 1988* are available on the Office's web site at www.privacy.gov.au.

Health service providers are also encouraged to contact their professional body or association for further information on privacy in their profession.

For further information contact:

Office of the Federal Privacy Commissioner

- 1300 363 992 (Hotline)
- privacy@privacy.gov.au
- www.privacy.gov.au