Guidelines on Privacy in the Private Health Sector

Office of the Federal Privacy Commissioner

8 November 2001

Foreword

The Privacy Amendment (Private Sector) Act 2000 extends the operation of the *Privacy Act 1988* to cover the private health sector throughout Australia.

The co-regulatory approach offered by the legislation allows for flexibility in how organisations (including health service providers) deal with their privacy obligations, while ensuring standards apply to the protection of personal information, including health information. The legislation recognises the particularly sensitive nature of health information, and places extra protections around its handling, including enforcement mechanisms to deal with breaches of the privacy standards.

In the private health sector, the legislation will complement the existing culture of confidentiality that is fundamental to many health service providers' professional practice obligations.

The legislation, through its ten National Privacy Principles, promotes greater openness between health service providers and consumers regarding the handling of health information. The legislation introduces, for instance, a general right of access for consumers to their own health records, and requires health service providers to have available documentation that clearly sets out their policies for the management of personal information.

Clear and open communication between the health service provider and health consumer is integral to good privacy. This document recognises that when such communication occurs, then ordinarily, many of the privacy obligations of health service providers will be met. When providers are open about the health information they hold, and how they use and disclose it, surprises are unlikely and with fewer surprises there are likely to be fewer complaints.

The recent research on community attitudes toward privacy, conducted by the Office, shows the importance Australians place on controlling their health information, even when used in relation to their treatment.

The guidelines acknowledge that the health service provider's principal concern is the health care of the patient. The Privacy Act realises individuals' wishes to have their privacy protected. Therefore, the guidelines aim to assist health service providers to meet their obligations under the National Privacy Principles while providing treatment and care.

The document aims to assist the private health sector in better understanding the application of the National Privacy Principles to its business and services. The document is supported by Information Sheets on the application of the Privacy Act in a number of other areas. These are available on the Office's website at www.privacy.gov.au. Health service providers are also advised to refer to information and advice on privacy from their respective professional bodies.

Malcolm Crompton
Federal Privacy Commissioner
October 2001

Quick Reference Guide

TABLE OF CONTENTS

PART A

A.1 Introduction

A.1.1 New privacy legislation for the private sector

In Australia, for the first time, there is now a comprehensive privacy law covering the private sector. In an amendment to the *Privacy Act 1988* (the 'Privacy Act'), private sector organisations now have an obligation to protect the privacy of individuals' personal information.

This amendment applies to all health service providers in the private sector, regardless of size, from 21 December 2001.

Most people consider health information to be highly personal, and therefore need to be confident that their privacy will be protected whenever they use a health service. The Privacy Act offers privacy protection to individuals and, at the same time, balances this with the legitimate need for health service providers to share information in order to facilitate the provision of quality health care.

The privacy legislation covers a wide range of information handling practices, including:

- needing to gain consent for the collection of health information;
- what to tell individuals when information is collected;
- what to consider before passing health information on to others;
- the details that should be included in a health service provider's Privacy Policy;
- securing and storing information; and
- providing individuals with a right to access their health records.

The provisions in the Privacy Act are based around 10 National Privacy Principles (NPPs) that represent the minimum privacy standards for handling personal information. Enforcement of the Act is generally through resolution of individual complaints lodged with the Privacy Commissioner or a Code Adjudicator, and sometimes through the Privacy Commissioner launching an investigation. The full text of the NPPs is included at Appendix 1.

A.1.2 Status of these guidelines

Under the Privacy Act, the Privacy Commissioner has power to issue guidelines. These guidelines are advisory, and are issued under section 27(1)(e) of the Privacy Act.

The guidelines are not legally binding; they aim to help health service providers comply with the NPPs and avoid interfering with the privacy of individuals. Nothing in the guidelines limits how the Commissioner will handle complaints.

A.1.3 Complaint-handling

If an individual thinks a health service provider has interfered with their privacy they can complain to the Privacy Commissioner. When the Privacy Commissioner receives a complaint the individual must in most cases be referred back to the provider to give the provider a chance to resolve the complaint directly (see s.40(1A) of the Privacy Act).

If the individual and the provider cannot resolve the complaint between themselves, the Office of the Federal Privacy Commissioner conciliates the complaint using letters and phone calls, or in some cases, face-to-face meetings. In the majority of cases, the complaint is resolved this way. As a last resort, the Privacy Commissioner can make a formal determination. If a health service provider does not comply with the determination either the Privacy Commissioner or the complainant can seek to have it enforced by the Federal Court. The Privacy Commissioner may also investigate an act or practice that may be a breach of privacy even if there is no complaint (see s.40(2) of the Privacy Act).

For further information to assist in preparing for the commencement of the new privacy provisions see the following:

- *Information Sheet 1 – 2001 Overview of the Private Sector Provisions*
- *Information Sheet 2 – 2001 Preparing for 21 December 2001*, and
- *Information Sheet 12 – Coverage of and Exemptions from the Private Sector Provisions.*

A.2 Who are these guidelines for?

A.2.1 Health service providers in the private sector

These guidelines are for private sector or non-government organisations that provide a 'health service'.

The term 'health service' is defined in the Privacy Act – see Appendix 2, *Definitions from the Privacy Act 1988*. Given the breadth of this definition, providers of health services range from hospitals, pharmacists and general practitioners to gyms and weight loss clinics.

In these guidelines, organisations that provide health services are referred to as 'health service providers'. The guidelines have been developed primarily with the following types of health service providers in mind (this is not an exhaustive list):

- private hospitals and day procedure centres;
- private aged care facilities;
- general practitioners and other medical practitioners, including medical specialists working in private practice;
- nurses, midwives, nurse practitioners and clinical nurse consultants;
- pharmacists;
- other health and allied health professionals in private practice including psychologists, physiotherapists, dentists, podiatrists, occupational and speech therapists and optometrists;
- pathology and radiology services;
- complementary medicine practitioners, including herbalists, naturopaths, massage therapists, nutritionists, and traditional Chinese medicine practitioners;
- chiropractors and osteopaths
- health services provided in the non-government sector, such as phone counselling services or drug and alcohol services;
- Aboriginal community controlled health organisations;
- blood and tissue banks;
- assisted fertility and IVF clinics; and
- health services provided via the Internet (eg counselling, advice, medicines), tele-health and health mail order companies.

However, any health service provider, or organisation working closely with them, may choose to consult these guidelines.

These guidelines are also intended for health service providers working within larger, non-health environments, such as community dentists employed in schools and medical practitioners in prisons and detention centres.

The guidelines are intended as a reference to the new privacy legislation for health service providers. They offer discussion and explanation on a range of privacy issues. However, they cannot cover all circumstances faced by a diverse range of providers across the sector.

Health service providers' professional associations will, usually, be the best source of advice, as and when more complex privacy issues arise. 'Quick guides', such as those being developed by some professional associations, will provide important assistance on a day-to-day basis.

Tip for compliance

Each employee and contractor of a private or non-government organisation that provides a health service needs to be aware of their obligations, and those of the organisation, under the Privacy Act. These guidelines aim to assist in this regard.

A.2.2 Health service providers in the public sector

The new provisions in the Privacy Act do not cover Commonwealth, State and Territory public sector health service providers. Therefore, these guidelines do not cover such providers.

A.2.3 Health service providers that operate in both the public and private sectors

A number of health service providers work in both the public and private sectors. For example, medical practitioners who work in both public and private hospitals, and organisations contracted by government for some of their work, but which otherwise operate privately.

In general, when a provider works in the private sector, the Privacy Act applies, and these guidelines are relevant. When working in the public sector, the relevant Commonwealth, State or Territory laws apply.

Complexities arise when services are delivered through a mix of private and public sector providers across both private and public sector sites. For example, where public and private hospitals are co-located.

Where a private health service provider works within a public hospital, it is generally the case that the medical record remains subject to management by the public sector hospital, and therefore comes under relevant State/Territory legislation – regardless of clinical entries in those records by public or private sector providers.

However, if a private health service provider treats an individual in a public hospital, but retains records (including copies) in a private clinic or other place away from the public hospital, these records would be subject to the Privacy Act.

A.3 What information does the Privacy Act apply to?

A.3.1 Personal information

The Privacy Act only applies to 'personal information'. That is, information about an individual who can be identified, or whose identity could be reasonably ascertained, from the information.

Personal information must relate to a natural, living person. A 'natural person' is a human being as opposed to an entity recognised by the law as a 'legal person', such as a company.

The NPPs do not apply to de-identified information or statistical data sets, which would not allow individuals to be identified.

A.3.2 Health information

These guidelines are concerned with 'health information', which is a particular subset of personal information. Health information is personal information:

- about an individual's health or disability at any time (that is, past, present or future);
- about an individual's expressed wishes regarding future health services;
- about health services provided, or to be provided, to the individual;
- collected whilst providing a health service; or
- collected in connection with the donation or intended donation of body parts and substances.

'Health information' includes any information collected by a health service provider during the course of providing treatment and care to an individual, including:

- medical information;
- personal details, such as a name, address, admission and discharge dates, billing information and Medicare number;
- information generated by a health service provider, such as notes and opinions about an individual and their health;
- information about physical or biological samples, where it can be linked to an individual (for example, where they have a name or identifier attached); and
- genetic information, when this is collected or used in connection with delivering a health service, or genetic information when this is predictive of an individual's health.

Under the Privacy Act, higher privacy standards apply to the handling of sensitive information. Health information is one kind of sensitive information, and is subject to additional provisions.

A.3.3 Health information

The Privacy Act states that other types of 'sensitive information' include, information about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, professional or trade association membership, union membership, sexual preferences or practices, or criminal record.

For organisations that do not provide health services, the distinction between 'personal information' and 'sensitive information' is an important one, due to the higher privacy standards that apply to the latter.

This distinction is not so critical in the health context, as all personal information collected in the course of providing a health service (including the types of sensitive information listed above) is 'health information'. Therefore, the higher privacy standards apply to all personal information collected by health service providers in the course of providing a health service.

A.3.4 Information held in different forms

The NPPs are high-level principles and apply in a range of situations. They are not designed to be specific to a particular technical or administrative environment. The principles apply to health information held in any form, including paper, electronic, visual (x-rays, CT scans, videos and photos) and audio records.

A.3.5 Employee records

The Privacy Act does not apply to information held by an employer about its current and former employees, where that information is held in employee records and its use or disclosure relates to the employment relationships.

However, if an individual attends a health service provider in a personal capacity (and that provider is also their employer), the information collected would not constitute part of their employee record. Thus, the Privacy Act would apply to health information collected in this situation.

The Act applies to information held about applicants for employment who were unsuccessful, and who never entered into an employee relationship with the organisation.

The Act also applies to the records of employees of other organisations when health service providers handle them, such as in relation to workers' compensation claims.

A.3.6 Health information held before the commencement of the Privacy Act

The new provisions in the Privacy Act are effective from 21 December 2001.

Only some of the National Privacy Principles (NPPs) apply to information collected before 21 December 2001. These include NPP 4 (on data security), NPP 5 (on openness), NPP 7 (on identifiers), and NPP 9 (on transborder data flows).

NPP 6 (on access) also applies to information already collected, but only where that information is still in use, and if giving access would not pose an unreasonable administrative burden or expense on the health service provider.

For more guidance on how the NPPs apply to information a health service provider has already collected when the private sector scheme commences, see *Information Sheet 10 - 2001 Application of the Privacy Act to Information Already Held*

A.4 Other laws, codes and guidelines

A.4.1 Professional and ethical codes and standards

The confidentiality of individuals' health information is already strongly protected in the health sector – through the obligations health service providers have under professional and ethical codes of practice. The Privacy Act does not prevent these codes of practice from continuing to apply.

In some instances, these codes or professional obligations apply stronger privacy protections than the NPPs, as is appropriate in the health context.

In other areas, the NPPs contain additional requirements to those in some professional codes of practice, and may broaden the obligations of health service providers. For example, generally, the legislation obliges health service providers to give individuals right of access to their records.

A.4.2 Other legislation on health and privacy

There are also other Commonwealth, State and Territory laws which apply to health service providers and regulate how individual health information must be handled. To the extent that there are direct inconsistencies between Commonwealth and State or Territory laws, generally, the Commonwealth law will prevail.

A.4.3 General guidelines on the NPPs

The Privacy Commissioner has developed 'Guidelines to the National Privacy Principles' (the 'NPP Guidelines'), and Information Sheets, to explain how the NPPs apply to private sector organisations across a broader range of sectors beyond the health sector. The NPP Guidelines and Information Sheets are available on the Office web site, at www.privacy.gov.au.

Most health service providers should find the information they need regarding the NPPs and their privacy obligations in these guidelines, as they have been developed to advise specifically on health-related issues. However, the NPP Guidelines and Information Sheets may be useful if further information is required about how the legislation applies outside the health sector.

For example, *Information Sheet 9 - 2001 Handling Health Information for Research and Management* provides more information on health research issues.

A.4.4 Codes approved under the Privacy Act

The Privacy Act allows the Privacy Commissioner to approve codes to replace the NPPs, as long as they include privacy protections that are at least the equivalent of all the obligations within the NPPs. An organisation can subscribe to an approved code and so be bound by it.

For more information about privacy codes see the Privacy Commissioner's Code Development Guidelines available on the Office web site, at www.privacy.gov.au.

A.5 Consent to collection, use and disclosure of personal information

Consent is relevant to many decisions about how health information is collected, used or disclosed.

Consent is not, however, required by the Privacy Act in all situations. The circumstances in which consent may or may not be required are discussed in more detail in Part B of this document.

To give some background, this section briefly explains the notion of consent as it relates to the handling of health information.

This section explains:

- what consent is;
- the different ways in which consent may be sought; and
- when consent may be sought from someone other than the individual.

The Privacy Act states that, in the context of the NPPs, consent can be express or implied. Express consent is given explicitly, either orally or in writing. Implied consent is agreement that can be inferred from an individual's conduct.

Tip for compliance

If a health service provider has the consent of an individual to collect, use or disclose their health information, then the provider may work with the information within the limits of that consent.

A.5.1 Consent to the handling of personal information, not *to medical treatment*

Consent, as discussed in the Privacy Act and these guidelines, applies to decisions about how an individual's health information is handled. The Privacy Act does **not cover consent to medical or dental treatment.**

In practice, consent to the handling of information and consent to medical treatment often occur at the same time, though they are distinct authorities by the individual to do different things: to provide treatment and to use health information in particular ways.

A.5.2 Key elements of consent

The key elements to consent are:

- it must be provided voluntarily;

- the individual must be adequately informed; and
- the individual must have the capacity to understand, provide and communicate their consent.

Consent must be voluntary – the individual must have a genuine opportunity to provide or withhold consent; that is, they must be able to say 'yes' or 'no' without extreme pressure which would equate to an overpowering of will.

Consent must be informed – the individual must know what it is they are agreeing to. In other words, the individual needs to be aware of the implications of providing or withholding consent, having received the information in a way meaningful to them and appropriate in the circumstances.

The individual must have the capacity to provide consent – the individual must be capable of understanding the issues relating to the decision, forming a view based on reasoned judgment and communicating their decision.

A.5.3 Express or implied consent

The Privacy Act states that consent may be 'express or implied'.

Express consent – refers to consent that is clearly and unmistakably stated, and can be obtained either in writing, orally, or in any other form where the consent is clearly communicated.

As a general rule, if a health service provider needs or wants consent and is in doubt about whether an individual is giving consent or not, it is preferable to seek express consent.

Implied consent – there are situations when health service providers may reasonably rely on implied consent by individuals to handle health information in certain ways.

> For example, an individual presents to a medical practitioner, discloses health information, and this is written down by the practitioner during the consultation – this will generally be regarded as giving implied consent to the practitioner to collect the information for certain purposes. The extent of these purposes will usually be evident from the discussion during the consultation.
>
> Similarly, if a medical practitioner collects a specimen to send to a pathology laboratory for testing, it would be reasonable to consider that the individual is giving implied consent to the passing of necessary information to that laboratory.

Where there is open communication and information sharing between the health service provider and the individual, consent issues will usually be addressed during the course of the consultation. If the discussion has provided the individual with an understanding about how their health

information may be used, then it would be reasonable for the health service provider to rely on implied consent.

Where consent is required from individuals for the collection and use of data for public health purposes, such as in relation to the establishment and maintenance of a disease register, it may sometimes be appropriate to take the approach of giving individuals the opportunity to opt out of being included on the register. The use of this approach by a health service provider would only be appropriate where individuals are clearly informed about the option to opt out and this is prominently presented and easy to adopt.

A.5.4 Consent on behalf of an individual

An individual cannot give valid consent if they lack the capacity to make an informed decision.

An individual may be unable to give consent for a number of reasons, including because they:

- have limited decision-making capacity due to a cognitive impairment, such as dementia or a severe intellectual disability;
- are experiencing a temporary incapacity, perhaps during a psychotic episode, due to a temporary psychiatric illness, or because of severe distress;
- are a young child; or
- are in an emergency situation and unconscious or in distress.

A lack of decision-making capacity and privacy-related consent issues should not mean that individuals miss out on getting necessary health care, support and other services. Yet, neither should an individual's privacy rights be undermined unnecessarily by virtue of their inability to give consent.

There are complex issues to balance here, and a few factors to consider are:

Involve the individual in decision-making

Most people with disabilities are able to make their own privacy decisions and have the legal right to do so. Health service providers will need to ensure that privacy issues are discussed with the individual in a way that is understandable and comprehensible, to the greatest extent possible in the circumstances.

Moreover, even if an individual lacks legal capacity, they should be involved as far as is practical in decision-making processes.

Who may act on the individual's behalf?

When consent is required, and an individual lacks capacity, a health service provider may need to consider who can act on the individual's behalf. There may be a range of options, including:

- a guardian;
- someone with an enduring power of attorney that can be used in relation to the individual's health;
- a person recognised by other relevant laws, for example in NSW, a 'person responsible' under the NSW Guardianship Act (this may be an individual's spouse, partner, carer, family member or close friend); or
- a person who has been nominated in writing by the individual while they were capable of giving consent.

In situations where there is no one available to act for an individual, the health service provider may have to make decisions about appropriate handling of the individual's health information. Professional and ethical obligations and current accepted practices may provide guidance in these circumstances.

Children and young people

The Privacy Act does not specify an age after which individuals can make their own privacy decisions. Determining the decision-making capabilities of a young person can be a complex matter, often raising other ethical and legal issues. Health service providers will need to address each case individually.

Section 2.9, *Disclosure of health information to a responsible person,* gives further information on children and young people's competence to make privacy decisions about the disclosure of their records.

A.6 Key Concepts

Access
This involves a health service provider giving an individual information about themselves. Access may include inspecting personal information or having a copy of it.

Collection
A health service provider collects personal information if it gathers, acquires or obtains personal information from any source and by any means. Collection includes when a health service provider keeps personal information it has not asked for or it has come across by accident.

Disclosure
In general terms, a health service provider discloses personal information when it releases information to others outside the organisation. Disclosure does not include giving an individual information about themselves (this is 'access', see above).

Use
In general terms, use of personal information refers to the handling of personal information within an organisation, including 'the inclusion of information in a publication'.

A.7 Summary of NPP obligations for health service providers*

Collecting Information

- Only collect health information necessary for your functions or activities.
- Use fair and lawful ways to collect health information.
- Collect health information directly from an individual if it is reasonable and practicable to do so.
- At the time you collect health information or as soon as practicable afterwards, take reasonable steps to make an individual aware of:
    - why you are collecting information about them;
    - who else you might give it to; and
    - other specified matters.
- Take reasonable steps to ensure the individual is aware of the above points even if you collect information about them from someone else.
- Get consent to collect health information, unless an exemption applies.
- If it is lawful and practicable to do so, give people the option of interacting with you anonymously.

Storage and Maintenance

- Take reasonable steps to ensure the health information you collect, use or disclose is accurate, complete and up-to-date.
- Take reasonable steps to protect the health information you hold from misuse and loss and from unauthorised access, modification or disclosure.
- Take reasonable steps to destroy or permanently de-identify health information if it is no longer needed for any further purposes.

Use and Disclosure of Information

- Only use or disclose health information for the primary purpose of collection unless one of the exceptions in NPP 2.1 applies (for example, if it is for a directly related secondary purpose within the individual's reasonable expectations, if you have consent, or where there are specified law enforcement or public health and public safety circumstances).
- Only adopt, use or disclose a Commonwealth government identifier if particular circumstances apply that allow you to do so.
- Only transfer health information overseas if you have checked that you meet the requirements of NPP 9.

Access (by the individual) to information

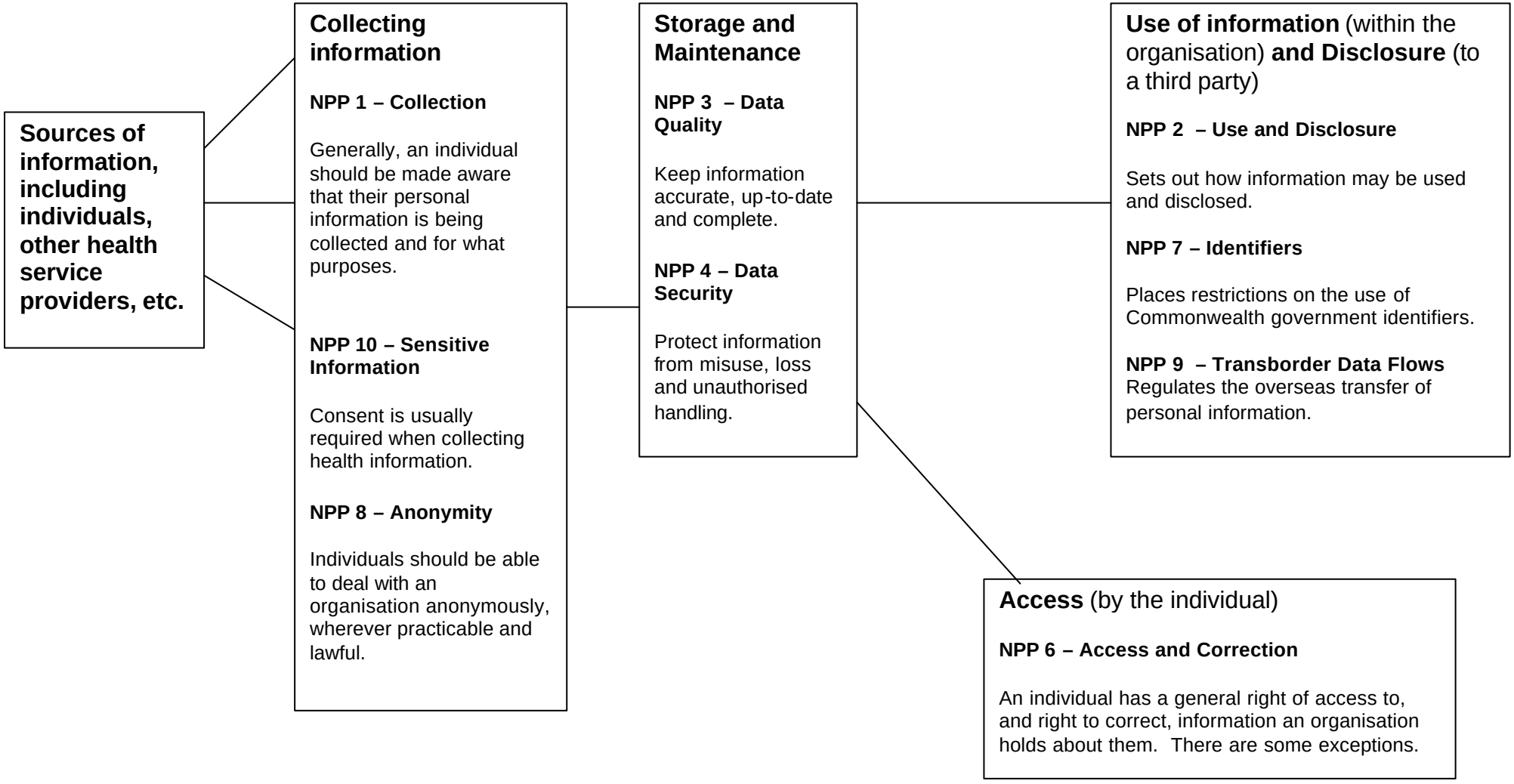
- If an individual asks, give them access to the health information you hold about them unless particular circumstances apply that allow you to deny access – these include where there is a serious threat to life or health.

Openness

- Have a short document that sets out your policies on how you manage health information. Make it available to anyone who asks for it.

*This is a summary only and NOT a full statement of obligations. These are set out in the NPPs themselves.

The National Privacy Principles and Health – Protecting privacy throughout the information life cycle



Openness **NPP 5 - Openness**

An organisation must have a document, such as a privacy policy, that informs about how it handles and protects personal information.

PART B

1 Collecting Health Information

National Privacy Principles 1 and 10

These principles set out a health service provider's obligations when collecting health information. These include:

- only collect personal health information with consent, except in specified circumstances including, but not limited to, emergencies, as required by law, or in circumstances relating to legal or equitable claims. A health service provider may also collect health information without consent, under special conditions, when providing a health service or when undertaking certain research or management activities;
- take reasonable steps to ensure that individuals are aware of certain matters, including, but not limited to, who is collecting the information, the fact that the individual is able to gain access to the information and the purposes for which the information is collected.
- only collect information necessary for the performance of the health service provider's functions or activities; and
- collect information directly from the individual where this is reasonable and practicable.

Health service providers collect health information about individuals from a number of sources, most often from individuals themselves. Information is collected for a range of purposes though predominantly for providing health care.

Both NPPs 1 and 10 regulate collection of personal health information. NPP1 covers collection of all personal information, while NPP10 places special conditions on the collection of sensitive information, including health information. From the perspective of health service providers, it is useful to consider these principles together.

1.1 What is collection?

Meaning of collection

A health service provider collects personal information if it gathers, acquires, or obtains it. Information about an individual is collected if a health service provider receives it directly from the individual, or from somebody else, and retains it. Information that a health service provider comes across by accident, or has not asked for, but nevertheless keeps, is also collected.

The NPPs apply equally to the collection of solicited or unsolicited health information.

Examples of collection include where a health service provider:

- writes down what an individual says, including any opinion about, or interpretation of, what is said;
- receives a form or a letter from an individual;
- re-identifies previously de-identified information;
- receives personal information via an electronic line for processing or further transmission;
- downloads and retains personal information from another computer server;
- receives personal information from another organisation under a contract to carry out an activity or provide a health service;
- stores video tapes or photographic images of procedures (e.g. colonoscopy) in ways that identify individuals; and
- receives and keeps emails containing personal information.

Collection occurs at the point where the health service provider first receives the information. Subsequent passing of information between staff within the health service provider organisation is 'use', and is discussed in Chapter 2. Collection also occurs where the provider obtains new information from or about the individual.

1.2 Collect only necessary information

NPP 1.1, NPP 10.1(c) & (e), NPP 10.2(a), NPP 10.3(a)

Information collected should be limited to what is necessary for the health service provider's functions and activities. This is of particular importance where information is collected without consent.

In assessing what is 'necessary', professional practice standards and obligations will be relevant.

This principle does, however, aim to limit situations where unnecessary information is collected, even unintentionally.

> For example, a hospital may have a form with spaces to collect much standard information, particularly where the form serves a number of purposes. Often, people may have the impression that they must fill in all fields, even if this is unnecessary.

1.3 Collecting information with consent

NPP 10.1(a)

A health service provider may only collect health information about an individual where they have that individual's express or implied consent to do so, or under certain other conditions described in the next section, *Collecting information without consen*t.

In situations where health information is collected directly from the individual, the individual's consent to the collection could generally be implied as long as it is clear to them what information is being recorded and for what purposes. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the health service provider.

1.4 Collecting information without consent

There are a limited number of situations where NPP 10 allows a health service provider to collect information about an individual without consent.

Professional rules of confidentiality of competent health or medical bodies

NPP 10.2

A health service provider may collect health information without an individual's consent when the collection is necessary to provide a health service, and where either the collection is carried out according to particular kinds of professional rules of confidentiality, or as required by law.

The rules dealing with obligations of professional confidentiality must be binding on the health service provider, and must be established by a competent health or medical body. Competent bodies might include medical boards and other rule-making bodies recognised in Commonwealth, State or Territory legislation. Binding rules are rules that must be followed, and generally, will give rise to some sort of adverse consequence if breached.

Laws requiring collection

NPP 10.1(b), 10.2(b)(i)

A health service provider can collect information without consent if there is a law requiring them to do so.

'Law' includes Commonwealth, State and Territory legislation, as well as the common law. Health service providers' legal obligations in this regard are generally set out in State and Territory legislation.

> For example, under a number of State and Territory public health Acts, health professionals are required to keep a record of certain details about an individual who they believe has a notifiable disease. Notifiable diseases include tuberculosis, Legionnaires' Disease and HIV/AIDS.
>
> Depending on jurisdiction, a health service provider may also be legally required to record certain details while providing health services, such as about an adverse event following immunisation.

Serious and imminent threats to life or health

NPP 10.1(c)

In situations where there may be a serious and imminent threat to the life or health of *any* person, a health service provider can collect, without consent, the information necessary to lessen or remove the threat.

This provision only applies where an individual is unable to provide or communicate their consent. This may include an emergency in which an individual is unconscious, or in significant distress or confusion, or otherwise unable to provide consent, and urgent treatment is required. This would include some acute psychiatric emergencies.

> For example, an individual is in hospital and unconscious as a result of a stroke. The hospital may need to contact the individual's general practitioner for relevant information. Where this information is necessary to lessen the threat to the individual's health or life, collection can occur.

(Section 2.4, *Serious threats to life, health or safety*, and Section 6.7, *Information withheld in some situations,* both provide further guidance.)

Information required for management, research or statistical purposes

NPP 10.3

This principle allows for collection related to management, research or statistics where it is impracticable to seek consent from the relevant individuals.

It applies where information is collected for research, or for the compilation or analysis of statistics, relevant to public health or public safety, or for the management, funding or monitoring of a health service. 'Management, funding or monitoring of a health service' may include some quality assurance and audit activities.

Health information may only be collected without consent for these purposes if seeking consent is impracticable, and de-identified information would not be sufficient. Where these preconditions exist, collection must be carried out either according to 'Section 95A Guidelines', or in accordance with binding

rules of confidentiality issued by a competent health or medical body, or as required by law.

> For example, a psychiatrist wishes to collect information from a mental health institution about a particular treatment used on patients 20 years ago, for the purposes of conducting research that relates to public health.
>
> In this example, it will be assumed that it is impracticable to seek consent from the individuals involved, and that de-identified statistical data would be insufficient. The psychiatrist could then make use of the provisions of NPP10.3, for example by following the Section 95A Guidelines.
>
> An example of collection for management, funding or monitoring of a health service would be an incident monitoring body, collecting information about dangerous incidents occurring in a private hospital.

For further information on this topic see *Information Sheet 9 - 2001 Handling Health Information for Research and Management*.

1.5 Advising individuals about information collected

NPP 1.3 and NPP 1.5

Advising the individual, at the time health information is collected, about how the health service provider will handle their information is an important part of protecting privacy.

Where health information is collected with consent, the advice given at the time of collection will also be important in ensuring that the individual is giving informed consent.

Where health information is collected without consent, the NPPs still require reasonable steps to be taken to inform individuals about how their information is to be handled.

Under NPP 1.3, when collecting personal information, including health information, a health service provider must take reasonable steps to ensure that the individual is aware of the following:

- the identity of the organisation and its contact details;
- that the individual may obtain access to their information;
- the purposes for which the information is collected;
- the organisations or persons to whom information is usually disclosed;
- any law that requires the information to be collected; and

- what the main consequences may be (if any) if the individual does not provide all, or part of, the information requested.

In some contexts this information may be obvious. For example, the name and address of the doctor collecting the information may be clear to the individual when that doctor is collecting it, in person, at their practice.

However, if the doctor is an employee of a large organisation, the identity of the organisation collecting the information may not be obvious to the individual.

Tip for compliance

The time at which information is collected is often the ideal time to seek consent from the individual about future uses of their information.

How to provide advice on these matters

According to NPP 1.3, 'reasonable steps' must be taken to 'ensure that the individual is aware of' the matters listed above.

What steps are reasonable, if any, will depend on the circumstances. In, many instances, such as when an individual visits their general practitioner, these steps will already occur as part of usual communication. Also, these issues usually only need to be addressed on a first visit by the individual, unless later changes to information-handling practices require that individuals be given updated information.

Thus, in many situations, a health service provider can inform the individual about how their information will be handled during discussion with them.

Another helpful method is to have a brochure or handout that provides general information on the health service provider's practices for handling and protecting health information.

> For example, a health service provider could develop a brochure for its clients on privacy and confidentiality. This could include information about how the organisation handles health information and how an individual can access their information. It could also advise on any laws that require information to be disclosed to government authorities.

Where a health service provider collects personal information on a form it could ordinarily satisfy its obligations under NPP 1.3 by including a statement on the form.

Where a health service provider collects personal information orally, a brief notice could be displayed, covering all relevant information, with the provider giving the individual more detailed information in a brochure.

Tip for compliance

Care is needed to ensure that information given to the individual is clear, understandable, and relevant to the circumstances.

If not practicable to advise at time of collection

NPP 1.3

There are situations where it may not be practicable to make the individual aware of all the matters listed earlier. If this is the case, reasonable steps should be taken as soon as practicable after the collection to notify the individual.

If a health service provider has limited time with an individual, they may choose (on balance with other health priorities) only to notify the individual, at the time, of the points most important to the individual in the context – this may be what is reasonable in the circumstances.

> For example, in an emergency situation there simply may not be time to provide, or the individual may not be in a fit state to comprehend, advice on how their information will be handled. As soon as is practical after the event, the individual should be given advice on the NPP 1.3 matters, including what medical information was collected, how it may be used and to whom it may be disclosed. This advice could be given, for example, in a brochure.

1.6 Collecting information lawfully, fairly and not intrusively

NPP 1.2

One of the requirements of this principle is that information must be collected by lawful and fair means, and this must not be done in an unreasonably intrusive way.

The principle reinforces a good practice approach to information collection.

Lawful collection

Essentially, for collection to be considered lawful, the manner in which information is collected must not breach any State, Territory or Commonwealth law.

> For example, ordinarily, it would not be 'lawful' to tape record a conversation or consultation without the individual's knowledge, as this is against the law in most States and Territories in Australia.

Fair collection

Collection of information is considered to be 'fair' if the approach taken is open and not misleading, and if the individual is not coerced into providing information against their will.

Intrusive Collection

An example of intrusive collection would be a situation when an individual is required to disclose delicate information where they can be easily overheard.

Tips for compliance

When a health service provider collects health information from an individual in a place where they may be overheard, such as a waiting room or open pharmacy, this should be done in a manner sensitive to the surroundings.

Some individuals may be particularly concerned or embarrassed about discussing health issues in an open or public area, so the provider may wish to take additional steps to make the individual more comfortable. For example, by talking so only the individual can hear what is said, or by taking the individual to one side, or by using a private room if one is available.

1.7 Collect from the individual where possible

NPP 1.4

Where it is reasonable and practicable to do so, a health service provider must collect information about an individual only from that individual.

Deciding whether or not it is reasonable and practicable to collect personal information directly from the individual depends on the circumstances and involves balancing a number of possible factors, including whether a reasonable person might expect their information to be collected directly or indirectly, how sensitive the information is and what is accepted practice (by consumers and the health sector).

When collecting health information from another source (other than the individual) NPP 10 still applies. This means that either the individual has consented to the indirect collection (either explicitly or impliedly), or collection without consent is allowable under NPP 10. Section 1.4, *Collecting without consent,* provides more information on this topic.

There are a number of situations where collecting health information directly from the individual may not be reasonable or practical, and the health service provider may need to collect information from another source. For example:

- in an emergency, where background health information is collected from relatives; or

- where a pathologist collects a specimen and accompanying information from a referring provider.

In circumstances where an individual lacks decision-making capacity and is in need of health services, a health service provider may need to collect information from others, such as carers. In some situations this could occur with the consent of a person representing the individual (Section A.5.4, *Consent on Behalf of an Individual*, may provide useful information.).

However, where there is no one to act for the individual, the provider may need to take decisions about collection in accordance with their professional and ethical obligations and current accepted practices.

What to advise individuals when information is collected from another source

NPP 1.5

In situations where information is not collected directly from an individual, they still need to be given advice about NPP 1.3 collection issues. (Section 1.5, *Advising individuals about information collected*, gives further guidance.)

This advice is not required if it would pose a serious threat to the life or health of any individual. Therefore, if a health service provider receives information about an individual, and determines that giving the individual advice about the matters set out at NPP 1.3 would pose a serious threat to the individual's own life or health or that of any other person, the provider does not have to give the advice.

If health information is collected from a third party, for example another health service provider, and the third party has informed the individual of the NPP 1.3 matters (as they relate to the health service provider now collecting the information), then no further notice is required.

Tip for compliance

When a health service provider collects information indirectly, they could ask the original collector to also advise about the NPP 1.3 information of the indirect collector.

Depending on the circumstances, this could mean that the health service provider that collects the information originally would need to include the name of the health service provider that is going to indirectly collect the individual's information, the fact that the individual can get access to that information, the purposes for which the collection occurs and to whom the indirectly collecting provider might give the information.

Where specialists (such as pathologists) collect information from a referring health service provider and do not personally see the individual, it may often be the case that the referring provider has gained consent (whether express

or implied) to the disclosure of the information to the specialist, and to the collection by that specialist for the purposes of the referral.

Tip for compliance

Where a health service provider, such as a pathologist, does not collect information directly from the individual, the pathologist could ensure the individual is aware of how their information will be handled (according to NPP1.3) via the referring provider. Alternately, the pathologist may decide to include this information with their bill or with their report from the referral.

Medical history-taking

Collecting information about an individual's family members, for example when taking a medical history, may involve collecting identifiable personal information about those people. In some circumstances, the NPPs may require that family members' consents be sought before collection occurs, and that they are informed of the collection. However, generally, this is not in line with the necessary and accepted practice of medical history-taking.

The Privacy Commissioner will ensure that the necessary collection of family medical history information can continue through the use of other provisions in the Privacy Act.

2 Use and Disclosure

National Privacy Principle 2

This principle sets out a health service provider's obligations when using and disclosing personal information. These include:

- only use or disclose personal information for the primary purpose for which it was collected, or for directly related secondary purposes if these fall within the reasonable expectations of the individual, unless another exception under this principle applies;
- only use or disclose personal information in other ways if the individual gives consent (whether express or implied), or if one of the exceptions to this principle applies. The exceptions include, but are not limited to, uses or disclosures required or authorised by law, those necessary to prevent or lessen a serious or imminent threat to someone's life, health or safety, or for research provided certain conditions are met; and
- make a written note of any use or disclosure with regard to a law enforcement body, under NPP2.1(h).

The principle also deals with other matters, including when a health service provider can disclose health information to a 'person responsible' for an individual who cannot give or communicate their consent.

This principle provides a framework for how a health service provider can use or disclose personal information. A *use* refers to the handling of information within an organisation while a *disclosure* refers to the transfer of information outside the organisation.

The importance of health service providers sharing personal information in many circumstances, during the provision of health services, is widely accepted by the community. In the health sector, the flow of personal information usually occurs in accordance with concepts such as sharing within the 'treating team' or 'on a need to know basis'. For many health service providers, the use and disclosure of personal information is already bound by the codes of practice or rules of confidentiality of their professions.

The Privacy Act provides for the continuation of necessary information handling practices in the health sector, within the new privacy scheme, through the combination of the primary purpose of collection, directly related secondary purposes, and consent to other uses and disclosures of health information. This combination is explained in more detail below.

The key to making this principle easy to meet is ensuring alignment between the expectations and understanding of the health service provider and those of the individual about what will be done with personal information collected.

Providers need to pay most attention to those circumstances where expectations are not shared.

Tip for compliance

Is there alignment between the health service provider's intentions and expectations for the use and disclosure of the information and those of the individual? If uncertain, the health service provider should check with the individual.

2.1 The Primary Purpose and Directly Related Secondary Purposes

NPP 2.1(a)

This principle allows health service providers to use and disclose personal information in relation to the primary purpose for which it was collected, and directly related secondary purposes within the individual's reasonable expectations. These uses and disclosures can proceed without further consent from the individual. However, there will ordinarily be a strong link between what an individual has been told (about the proposed uses and disclosures) or has given consent to, and their 'reasonable expectations'.

The primary purpose is the main or dominant reason a health service provider collects information from an individual. Having a carefully determined primary purpose is part of privacy-sensitive, holistic health care.

Determining the primary purpose of collection should always be possible. When an individual provides, and a health service provider collects, personal information, they usually do so for a particular purpose; this is the primary purpose of collection – even if the health service provider has other additional purposes in mind.

When a health service provider collects personal information directly from an individual, *the context* in which collection occurs will assist in settling the primary purpose. When a health service provider collects personal information about an individual *from someone else*, the provider will often need to use or disclose it soon afterward. This use or disclosure offers a guide to the primary purpose of collection.

The concept of holistic health care recognises that a health service provider can treat an individual for a number of different complaints or ailments at a single time. In these circumstances, the primary purpose is linked to each of these conditions or ailments.

This principle also allows personal information to be used or disclosed without further consent if this occurs for reasons directly related to the primary purpose and these are within the reasonable expectations of the individual. These are uses and disclosures for **directly related secondary purposes**.

A reasonable expectation in these circumstances is what a reasonable individual with no special knowledge of the health sector would expect to happen to their health information. When an individual talks about the types of uses and disclosures they expect regarding their personal information, this will generally need to be taken into account when determining 'reasonable expectations'.

Implications for health service providers

In general, then, health service providers can proceed as usual, but need to take care not to go beyond the expectations of the individual. If a provider is uncertain, they could try to make sure the individual understands and expects the proposed uses and disclosures or they could explicitly seek consent.

In most situations, an individual's expectations will be apparent through normal communication. Where the individual's expectations are reasonably clear, and the health service provider works within them, there are likely to be less privacy problems.

In the course of open communication between the provider and the individual, consent to collect health information is often implied, the expectations of the individual are better understood, and the individual may give consent to a range of other uses and disclosures necessary for further health care.

Tips for compliance

When determining the primary purpose, health service providers should recognise that some individuals want to use health services in particular and limited ways. For example, the individual who goes to a sexual health centre seeking assistance in relation only to specific sexual health issues.

When determining 'reasonable expectations', considerations for health service providers include the individual's age, gender or cultural, linguistic and socio-economic background.

Expectation is more than awareness – telling someone about proposed secondary uses or disclosures may not necessarily create a reasonable expectation. A health service provider should consider the kind of person they are talking to, what their understanding is likely to be and therefore what they may reasonably expect. Indeed, if an individual expresses negative views, when made aware of a proposed secondary use or disclosure of their personal information, this would ordinarily indicate that they would not reasonably expect that use or disclosure to occur.

Sharing information with other health service providers: primary purpose, directly related secondary purposes or with consent

The multi-disciplinary team approach to health care is common to the Australian health system. Under this approach practitioners work together

and share necessary information, usually in accordance with codes of practice, to deliver optimum patient care.

Health service providers involved in care and treatment for the **primary purpose** and/or **directly related secondary purposes** would usually not need to seek further consent for necessary uses and disclosures. This will, however, depend on the circumstances of the case and the needs and wishes of the individual.

> For example, an individual goes into hospital for an operation. Generally, uses or disclosures necessary to carry out the operation (including, information sharing with pathologists, radiographers or anaesthetists) are integral in delivering the health service. Further consent is not needed where the individual reasonably expects this approach.

Other examples of necessary information sharing, which would usually fall within reasonable expectations are:

- after an individual agrees to see a specialist, necessary information sharing between the general practitioner and specialist;
- review of specimens by a senior pathologist on request from a junior pathologist to determine a diagnosis; and
- wards rounds and team-based case reviews.

Some individuals want or need to use health services in specific ways. For instance, someone may seek care and treatment through a particular health service provider, wanting to tell certain information *only to that provider*. Therefore, it is likely there will be circumstances where a health service provider needs to seek consent before sharing information with another provider. This may include some second opinions.

When collecting information, it may be advisable to discuss with the individual how the team-based approach to treatment will affect the handling of personal information.

Information on other directly related secondary purposes in the health sector

Directly related secondary purposes may include many activities or processes necessary to the functioning of the health sector.

Where the use or disclosure of de-identified data will not suffice, and provided it is within the reasonable expectations of the individual, no extra steps need be taken when using or disclosing relevant personal information in circumstances, such as:

- providing an individual with further information about treatment options;
- billing or debt-recovery;

- an organisation's management, funding, service-monitoring, complaint-handling, planning, evaluation and accreditation activities – for example, activities to assess the cost effectiveness of a particular treatment or service;
- disclosure to a medical expert (only for medico-legal opinion), insurer, medical defence organisation, or lawyer, solely for the purpose of addressing liability indemnity arrangements, for example in reporting an adverse incident.
- disclosure to a lawyer for the defence of anticipated or existing legal proceedings;
- an organisation's quality assurance or clinical audit activities, where they evaluate and seek to improve the delivery of a particular treatment or service; and
- disclosure to a clinical supervisor by a psychiatrist, psychologist or social worker.

Tip for compliance

Good privacy would include referring to these types of activities in the health service provider's information handling statements or brochures.

Health service providers will be in a better position to assume that such activities are within the reasonable expectations of an individual, if there has been appropriate education for the community about the activities.

2.2 Other Secondary Uses and Disclosures, not directly related

Many other secondary uses and disclosures will best be authorised by consent (whether express or implied). However, the principle also allows for some uses and disclosures, without consent, in limited circumstances. These are discussed in the sections below.

Note: NPP2 provides for the disclosure of health information with or without consent, in particular circumstances, as listed in the exceptions to the principle. However, in the absence of a *legal requirement* to do so, nothing in NPP 2.1 obliges a health service provider to disclose personal information. Professional codes of practice will generally offer guidance in these circumstances.

2.3 Uses and Disclosures with Consent

NPP 2.1(b)

A health service provider can use or disclose personal information for almost any purpose if they have the consent of the individual.

This section discusses some of the uses and disclosures for which consent is most likely to be necessary.

Training and Education

It is important for health service providers to be able to train in 'real life' environments. Training and education, in some cases, may be as effective by using de-identified case studies, or in the case of IT training through using simulated data. If a health service provider uses de-identified information for training, consent is not required.

Where the use of health information is necessary for training purposes, the sensitivity of such information needs recognition as some individuals seeking health care may not want their information disclosed any more widely than is necessary to receive care. These individuals may not want their information used for training or education activities.

The use of information for training and education will therefore usually require the individual's consent.

Tips for compliance

Whether consent is needed may depend on the nature of the training activity and the expectations and wishes of the individuals involved.

Intrusive training activities, or those less closely linked with service provision, are more likely to require express consent. For instance, videotaping a family therapy session, when the identities of participants will be revealed, is highly likely to require express consent.

Where consent is sought, the individual should have a genuine choice and not be pressured to participate. The individual should be told about the specific nature of the activity and the student group involved.

Media

Ordinarily, the disclosure of personal information to the media by a health service provider is not permitted without consent.

Examples of media requests to health service providers include:

- an accident or suspected crime, where the media is interested in the extent or nature of the injuries sustained by those involved, particularly if a person of public notoriety may be involved; or
- where there is a negligence claim against a health service provider and the media seeks a public interest story.

Tip for compliance

Information could be released to the media if it would not identify any individual, and not allow them to be identified from details about the incident or surrounding circumstances. However, even generic statements may identify a person in some circumstances.

Fundraising

Ordinarily, information collected by a health service provider during the provision of health services cannot be used for fundraising without consent

A health service provider could only use personal information for fundraising, if it was collected primarily for that purpose.

For example, a fund raising section of a private hospital may want to write to former patients asking for donations. The section wishes to use only names and addresses to do so. However, an individual's name and address, collected in the course of providing a health service, is regarded as 'health information'. Seeking donations using this information would not be a directly related secondary purpose, nor within reasonable expectations. The hospital would need consent to use the information in this way.

Direct marketing

NPP2.1(c) provides for the use or disclosure of personal information, for direct marketing without consent, in certain circumstances. This provision does not apply in relation to sensitive information including health information, and therefore is not open to health service providers.

Ordinarily, direct marketing using health information would not fall within the reasonable expectations of most individuals.

Tip for compliance

Care should be exercised with uses and disclosures that may be seen as direct marketing, and consent sought if the nature of the circumstances is unclear.

Transferring records to another health service provider on request

If an individual wants to transfer their care to another health service provider, they can authorise the disclosure of health information from the original provider to the new provider. A copy of this information could be transferred in this way.

However, if the original provider declines to transfer the information, then under NPP 6 the individual may request access to the health information and seek a copy. Unless an exception under NPP6 applies, the provider is obliged to give a copy of the record to the individual, who can then take it to the new health service provider.

2.4 Use and disclosure necessary for research and statistics relevant to public health or public safety

NPP 2.1(d)

In limited circumstances, this provision allows uses or disclosures of health information for research purposes, or for the compilation or analysis of

statistics without consent, where these activities are relevant to public health or public safety. That is, the research must be about, or the statistics related to, public health or safety.

Health information may be used or disclosed without consent for these purposes, only if:

- the activities cannot be undertaken with de-identified information and they are relevant to public health and safety;
- seeking consent is impracticable;
- the activities are carried out in accordance with guidelines that are developed by the National Health and Medical Research Council (or a prescribed authority) and are approved by the Privacy Commissioner; and
- for disclosure – the health service provider reasonably believes that the organisation to which they disclose will not further disclose the health information or any personal information derived from it.

When deciding whether a use or disclosure is 'necessary' for research or statistics, a health service provider must consider whether employing de-identified information would be sufficient. If de-identified information would suffice, the provider cannot use this principle to justify using identified information.

Whether it is impracticable to seek consent will depend on the particular circumstances of the case. Simply incurring some expense, or having to exercise some effort to seek the consent of individuals whose information is to be used or disclosed, would not ordinarily make it 'impracticable' to seek consent. Circumstances where it may be impracticable to seek consent could include where there are no current contact details for the individuals in question and where there is insufficient information to get up-to-date contact details. This might occur in longitudinal studies of old records.

Tip for compliance

It is advisable to include some information in the health service provider's information handling policies or patient brochures if the provider is regularly involved in these kinds of research projects. This may assist in advising individuals who use the service about how their data may be used or disclosed for research activities.

For further information on this topic see *Information Sheet 9 - 2001 Handling Health Information for Research and Management*.

2.5 Serious threats to life, health or safety

NPP 2.1(e)

In limited circumstances, a health service provider may need to use or disclose personal information to lessen or prevent:

- a serious and imminent threat to an individual's life, health or safety; or

- a serious threat to public health or public safety.

This exception allows for such uses and disclosures and generally relates to emergencies. Depending on the circumstances, this exception can allow disclosures to the police service or other government authorities, such as a community services department or mental health crisis team. The exception also allows for disclosure to an individual whose life, health or safety is threatened.

A 'serious and imminent' threat to an individual's life, health or safety relates to harm that could be done to any person (including the individual seeking treatment and care).

A 'serious' threat must reflect significant danger, and could include a potentially life threatening situation or one that might reasonably result in other serious injury or illness. Alternatively, it could include the threat of infecting a person with a disease that may result in death or disability. A threat could also relate to an emergency, following an accident, when an individual's life or health would be in danger without timely decision and action.

A threat is 'imminent' if it is about to occur. This test could also include a threat posed that may result in harm within a few days or weeks. It is much less likely to apply to situations where the risk may not eventuate for some months or longer.

A 'serious' threat to public health or public safety relates to broader safety concerns affecting a number of people. This could include the potential spread of a communicable disease, harm caused by an environmental disaster or harm to a group of people due to a serious, but unspecified, threat.

2.6 Use and disclosure regarding suspected unlawful activity

NPP 2.1(f)

This provision recognises the legitimate function of an organisation, including a health service provider, in investigating (internally) and reporting suspected unlawful activity. Usually, but not in all cases, the suspected unlawful activity would relate to the operations of the health service provider.

Such investigations may include the internal handling of complaints or allegations regarding professional misconduct, sexual harassment or assault and the reporting of them to the police or another relevant person or authority.

For further guidance on this topic see *Information Sheet 7 – 2001 Unlawful Activity and Law Enforcement*.

2.7 Use or disclosure required or authorised by law

NPP 2.1(g)

The Privacy Act recognises other legal obligations to use or disclose personal information. 'Law' in this context includes Commonwealth, State and Territory legislation, and the common law.

If the law *requires* that a health service provider use or disclose information, the provider must do so. Examples of such requirements include the mandatory reporting of child abuse (under care and protection laws) or the notification of diagnoses of certain communicable diseases (under public health laws).

Disclosure must occur if there is a warrant or law requiring the health service provider to do so.

If the law *authorises* the use or disclosure of information, the health service provider can decide whether to do so or not – the legal authority exists, but the provider has discretion.

Tips for compliance

The Privacy Act does not compel a health service provider to use or disclose personal information, but other law may do so.

Where a use or disclosure is authorised by law, health service providers' professional codes of practice and ethics may offer relevant guidance.

Other disclosures in the health and welfare sectors, under this provision, would include those to guardians or administrators (depending on the decision-making powers conferred upon them) and to guardianship, administration and mental health tribunals.

For further guidance on this topic see *Information Sheet 7 – 2001 Unlawful Activity and Law Enforcement*.

Courts and legal proceedings

At times, health service providers may be called to disclose health information to Courts or Tribunals.

If served with a subpoena or other form of Court order requiring the production of documents to the Court, a health service provider is generally required by law to provide the documents identified in the order.

However, Court orders may be challenged and may not require production of all documents held by a health service provider (such as those for which legal professional privilege may be claimed by the provider). If a health service provider has concerns about the information required to be produced by a Court order, or is unsure how to proceed, they could seek advice via the

Registrar of the Court or Tribunal which issued the order, a legal adviser or their professional body.

2.8 Use and disclosure and enforcement bodies

NPP 2.1(h)

This provision permits a health service provider to use or disclose personal information, where they have a reasonable belief that this is reasonably necessary for a range of functions or activities carried out by, or on behalf of, an enforcement body. An enforcement body in this context includes the National Crime Authority, the Australian Customs Service and other Commonwealth, State or Territory authorities established under law to conduct criminal investigations or inquiries.

Permitted uses and disclosures could relate to suspected unlawful activity, criminal offences or other breaches of law, suspected improper conduct or preparation for and conduct of Court or Tribunal proceedings. This is not an exhaustive list; refer to NPP2.1 (h) for more information.

The Privacy Act does not intend to interfere with health service providers' legal obligations, which might already affect the use and disclosure of personal information. For example, this provision does not override the duty of confidentiality between a medical practitioner and an individual. A health service provider is entitled not to disclose personal information if there is no law that requires it.

However, the Privacy Act does not intend to deter health service providers from lawfully co-operating with agencies performing law enforcement functions. Police and other enforcement bodies are generally reliant on voluntary co-operation to provide information.

Many health service providers, including mental health or drug and alcohol workers, general practitioners and counsellors, treat people who engage in unlawful activity. These individuals need to have access to health services in confidence, particularly for treatment of health issues intrinsically linked to unlawful behaviour. Usually, this approach sits at the core of the 'harm minimisation' model in dealing with a range of 'at risk' behaviours.

When considering a request for such a disclosure, the importance of maintaining the individual's confidentiality must be balanced with the public interest in the investigation and enforcement of the criminal law.

Tips for compliance

Before deciding to use or disclose health information under this provision, health service providers should consider:

- the seriousness of the situation – for instance, an investigation into an alleged murder or sexual offence would be more serious than property theft;

- the risks associated with a disclosure without the individual's consent or knowledge, balanced against the implications of non-disclosure;
- their relevant professional and ethical obligations; and
- whether the circumstances indicate a serious and imminent threat to the health, life or safety of any person.

If a health service provider discloses information under this provision, the Privacy Act requires that a written record be kept.

The NPP Information Sheet on *Law Enforcement and Regulatory Activity* has more information on this issue.

2.9 Disclosure of health information to a responsible person

NPP 2.4, 2.5 and 2.6

These provisions allow for the disclosure of health information by a health service provider to a 'person responsible' for an individual (including a partner, family member, carer, guardian or close friend), if that individual is incapable of giving or communicating consent.

Disclosure can occur:

- because it is necessary for the provision of appropriate care or treatment to the individual; or
- for compassionate reasons.

The disclosure should be limited to the information that is reasonable and necessary to achieve either of the above purposes.

Disclosure cannot occur if this is contrary to wishes expressed by the individual before losing the ability to give or communicate consent, and the health service provider is aware, or could reasonably be expected to be aware, of these wishes.

> A disclosure necessary for care or treatment could include an occupational therapist telling a sibling, who provides care in the home, about aspects of an individual's current physical condition. The information might cover limitations to the individual's physical and cognitive abilities, in order to explain how to carry out certain personal care tasks.
>
> A disclosure for compassionate reasons could include a doctor telling an individual's partner about the extent of the individual's injuries and their prognosis following a car accident.

The Privacy Act defines a 'person responsible' as:

- a parent of the individual;
- a child or sibling of the individual, who is at least 18 years old;
- a spouse or de facto spouse of the individual;

- a relative of the individual who is at least 18 years old and a member of the individual's household;
- a guardian of the individual or a person exercising an enduring power of attorney granted by the individual that can be exercised in relation to the individual's health;
- a person who has an intimate personal relationship with the individual; or
- a person nominated by the individual to be contacted in an emergency.

Tips for compliance

Professional judgement will assist when deciding if someone is a 'person responsible' – considerations will include the nature of the relationship between the person and the individual.

Depending on the circumstances, 'a person who has an intimate personal relationship with the individual' may include a same-sex partner, someone in a close relationship or friendship with the individual, or a companion or carer of the individual.

The Privacy Act does not specify that a parent must be a 'custodial parent'. This allows flexibility in judgement when determining to whom to disclose information.

In determining whether to disclose information to a 'person responsible', a provider will need to consider whether this would be contrary to any known wishes of the individual (previously expressed), whether it is necessary for care and treatment or is for compassionate reasons.

Disclosure of information to a 'person responsible' does not, in itself, represent an entitlement for that person to make health care or medical treatment decisions for the individual.

Where an individual has no one to act on their behalf, a health service provider may need to decide how best to use and disclose the individual's health information, to ensure they gain necessary treatment, care and services. Health service providers' professional and ethical obligations and standards of accepted practice are likely to offer guidance in these circumstances.

However, this principle does not provide the basis for disclosure to other service providers, organisations or professional carers. Section 2.1, *The Primary Purpose and Directly Related Secondary Purposes: Sharing information with other health service providers*, includes further information about these sorts of disclosures.

Disclosure and the records of children and young people

This provision recognises that, where a child or young person is not competent to make their own privacy decisions, a health service provider can discuss the young person's health information with a parent. Where the health service provider considers it appropriate, this may include showing the child or young person's health record to a parent.

However, in circumstances where a young person is capable of making their own decisions regarding their privacy, they should be allowed to do so.

Determining competence can be complex, and will lead to the health service provider having regard to the young person's maturity and their understanding of the relevant circumstances. There will be younger persons, in certain circumstances, who have attained sufficient competence (maturity and understanding) to make their own decisions. Conversely, there may be older teenagers who lack such competence. Health service providers will need to deal with each case subject to its circumstances.

Tips for compliance

Judgements about a young person's competence could involve consideration of their ability to understand the current issues and circumstances, their maturity and degree of autonomy, and the type and sensitivity of the information to be disclosed.

Existing laws covering health service providers' obligations in relation to children or young people and their confidentiality vary between States and Territories. These laws may offer further guidance in determining a young person's competence.

If the young person is not competent, their views should still be considered; so too, the risks and benefits of disclosure in the circumstances. A parent will not necessarily have a right to their child's information.

Complexities arise when a parent seeks information about their child, but the child explicitly asks that certain health information not be disclosed to that parent. For instance, a child may reasonably be seeking health services in confidence, to address drug and alcohol, sexuality, suicide, depression and other mental illness or pregnancy issues. The provider may consider it appropriate, in the circumstances, to keep such a confidence.

In exceptional cases, a health service provider may also decide not to disclose health information collected from a much younger child. This would generally relate to a risk of serious and imminent harm posed to the child, or others, if disclosure took place. For example, if a parent is abusive toward a child or other family members, a health service provider may decide there are reasonable grounds to believe a disclosure of the child's health information would result in greater danger.

3 Data quality

National Privacy Principle 3

Under this principle health service providers must take reasonable steps to ensure that the personal information they collect, use or disclose is accurate, complete and up-to-date.

Health service providers need to take reasonable steps to ensure the integrity of personal information when they collect, use or disclose it. However, providers are not required to check all data continually.

Benefits in maintaining quality health information can include its reliability in supporting informed decisions about health care and treatment and its role in facilitating the continuity of care when a new health service provider becomes involved, whether temporarily or permanently. Risks relating to poor data integrity can include the misrepresentation of an individual's health condition.

Tips for compliance

Health service providers are encouraged to think about where inaccuracy, incompleteness and lack of currency of personal information will most likely detrimentally affect individuals.

Factors to consider when determining 'reasonable steps' to ensuring data quality may include:

- the likelihood that the information in question is complete, accurate and up-to-date;
- whether the information changes over time;
- how recently it was collected;
- how reliable it is likely to be – this may include professional judgements about whether, or what, clinical information requires verification;
- who provided the information; and
- how it will be used.

If a health service provider uses information soon after collecting it from the individual, it probably does not need to be checked. If the information is collected from another source, the need to confirm its integrity may increase.

Where information is not in use (for instance, if it is stored in archives), it would generally be reasonable to take no action in relation to the standards in this principle.

4 Data security

National Privacy Principle 4

This principle requires that a health service provider take reasonable steps to:

- protect the health information it holds from misuse and loss, as well as from unauthorised access, modification or disclosure; and
- destroy or permanently de-identify health information that is no longer needed.

4.1 Data security

This principle requires a health service provider to have security safeguards in place to protect health information. These safeguards apply to personal information held in paper form, electronically, as film (such as x-rays) or photographs, and on audio or videotape (perhaps collected via tele-medicine).

If personal information is not securely stored and managed there is an increased risk of privacy breaches. Therefore, the principle requires that steps be taken to protect information against both accidental loss and intentional breach.

Practices that may lead to breaches of security include:

- leaving medical notes unattended at a public counter;
- not disposing of health records in a secure manner;
- inadequate controls regarding which staff can access health information – this might include inadequate password control on a database; and
- storing sensitive data on a laptop computer that is taken 'off-site' and not stored securely.

Tips for compliance

Determining reasonable security measures will depend on the circumstances. Relevant factors to consider could include:

- the sensitivity of the health information held by the health service provider;
- the harm likely to result if there is a breach of security;
- the form in which the information is stored (on paper, electronically or video), processed and transmitted; and
- the size of the organisation and the cost-effectiveness of the options available.

Examples of reasonable steps could include:

- implementing computer system safeguards, including password protection with required regular changes to passwords;
- providing lockable physical security for paper records;
- ensuring information is transferred securely (for example, not transmitting health information via non-secure e-mail); and

- monitoring information systems to test and evaluate data security.

Tip for Compliance

Health service providers can get additional assistance and information on data security from a range of sources. For example, providers could refer to relevant national standards such as AS/NZS ISO/IEC 17799:2001 and AS/NZS 7799.2:2000 developed by Standards Australia (more information can be found at www.standards.com.au).

For further guidance on this topic see *Information Sheet 6 – 2001 Security and Personal Information*.

4.2 Destruction or permanent de-identification of health information

This principle requires that information no longer needed for further uses or disclosures be destroyed or permanently de-identified. This information could include records no longer required for treatment and care, or for health service management, monitoring or evaluation, or for legal reasons.

Health information is highly valuable for many reasons, most importantly for an individual's on-going health care, but sometimes also for wider public health and safety reasons. Some State and Territory legislation, or guidelines issued by health professional organisations, require or recommend the retention of health information by health service providers for varying periods of time. Where there is a legal requirement to retain health information, this must be followed.

There is a need to balance, amongst other things, benefits to health care with privacy when deciding how to proceed with the destruction of health information. However, health service providers will need to consider the risks in keeping health information for longer than is necessary, as this may increase the risk of privacy breaches.

Tips for Compliance

Considerations regarding the retention or destruction of health information might include:

- legal or professional requirements to retain it;
- the benefits and risks of keeping the information;
- the likely significance of the information for the individual's future care or for future public health knowledge or research; and
- its possible importance in relation to new reproductive and genetic technologies.

Alternatives to destroying health information could be considered and may include, archiving data securely or keeping summary or statistical information, where this is sufficient.

5 Openness

National Privacy Principle 5

Under this principle, a health service provider must have a document that clearly sets out its policies on handling personal information. It must make this document available to anyone who asks for it.

On request, a health service provider must also take reasonable steps to let a person know what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

5.1 A privacy policy

An organisation is required to develop a document explaining its policies on handling personal information. This document is often referred to as a Privacy Policy.

The detail and length of the policy will depend on the size of the organisation.

The Privacy Policy can be made available in a number of ways, depending on what is most effective in the circumstances. For example, it could be:

- on a sign in a practice;
- in a printout or a pamphlet that could be handed out by the health service provider if someone asks for it; or
- for on-line services, on a website, either on a home page or on a prominent and accessible link from a home page.

When deciding how best to make the policy available, a key factor will be to ensure that individuals are able to readily access and as far as possible be able to understand the policy. For example, additional assistance or explanation may be needed for people whose first language is a language other than English, people with disabilities or for people with literacy difficulties.

As not all individuals have access to computer and internet facilities, a policy placed only on a website may not be sufficient and the provider may need to make the policy available in other forms.

Tips for Compliance

A large health service provider, such as a private hospital, may decide to provide a comprehensive policy, or alternately a number of related policies about different information systems or for different groups of individuals.

A smaller provider, such as a medical practice involving one or two practitioners, would be able to rely on a more straightforward policy explaining, in simple terms, how and what information is collected and the privacy safeguards the practice has in place to protect information.

What a health service provider decides to include in its Privacy Policy will depend on the type of health information it holds and how it manages that information. The Privacy Policy would at least need to cover:

- whether the health service provider is bound by the Privacy Act or a code approved by the Privacy Commissioner, and if this is the case, a reference to the code;
- any exemptions under the Privacy Act that apply to information the provider holds, or to any of its acts or practices; and
- that an individual can get more information, on request, about the way the provider manages personal information held.

Tip for compliance

Additional information that a health service provider could cover in a policy includes:

- the reasons certain types of information are collected;
- any routine procedures for collecting, holding and disclosing information, including if the provider contracts out such services;
- any laws that require the provider to disclose information to other organisations, such as government authorities;
- how requests for access to information are handled;
- the process a provider has in place for dealing with complaints about breaches of privacy under this Act; and
- the provider's contact details.

A health service provider also has obligations under NPP 1.3 to inform an individual, at the time of collection, about how their information will be handled. While a Privacy Policy can assist in meeting some of these obligations, other information is likely to be required around the time of collection, to fully satisfy this provision. (For more guidance, see Section 1.5, *Advising individuals about information collected.*)

5.2 Providing further information on request

This provision requires a health service provider, on request, to take reasonable steps to give an individual more detailed advice about the sort of personal information it holds, for what purposes, and how the provider collects, holds, uses and discloses the information. This could occur either by

the provider talking to the individual or by giving them more written information.

The steps that might be considered reasonable depend on the type of health service provider, its size, and how much information the individual wants. In some situations, providing a copy of the health service provider's Privacy Policy may be adequate to satisfy the individual's request. In other situations, a more detailed explanation may be required.

For further guidance on this topic see *Information Sheet 3 – 2001 Openness*.

6 Access and correction

National Privacy Principle 6

This principle sets out a health service provider's obligations regarding giving an individual access to personal information held about them. These include:

- giving an individual access to their personal information if they ask for it, unless particular circumstances apply that allow the health service provider to deny access or to limit the extent to which access is given – these circumstances include where there is a serious threat to life or health, specific business imperatives and occasions relating to law enforcement or other public interest matters;
- withholding access as required by law;
- when access might otherwise be denied, considering whether providing access through an intermediary is possible; and
- where reasonable, correcting personal information at the request of the individual.

This principle facilitates open communication between the individual and the health service provider by allowing individuals to access health information held about them, and individuals to correct that information if they believe it is not accurate, complete or up-to-date.

The right to access information under this principle only permits individuals to seek access to their own health records.

6.1 Forms of access

Access may be provided in a number of different ways. For example, an individual may:

- look at the information and talk though the contents with their health service provider;
- obtain a copy of the information (for example, a photocopy in the case of paper records, or a copy of an x-ray) or take notes on the content;
- listen to or view the contents of an audio or video recording; or
- obtain a print-out of the information if it is stored electronically, or be given an electronic copy of the information.

In the health sector, often it may be helpful to provide the individual with an opportunity to discuss their health information when access is sought. This may prevent the information being misunderstood or taken out of context. It may also save unnecessary hurt or distress for the individual if the information is potentially upsetting.

A health service provider is not obliged to re-format or summarise the material in response to an access request. However, if the health service provider believes a summary form may be more helpful and is willing to prepare one, and the individual wants the information in this form, this could be offered to the individual instead of, or as well as, the original record. Depending on the circumstances, the individual may only be seeking a summary of the record.

Where possible, access should be provided in the form requested by the individual. If an individual specifically requests a copy of the original record, this will need to be provided.

6.2 Requests in writing

It is not a legal requirement that requests be made in writing, and there are likely to be some situations where a written request is unnecessary. For example, if an individual asks a health service provider for a copy of their latest test results during the consultation, this request could be handled by simply providing a copy of the information at the time.

If the request is more complex, for example because it involves collating information from both paper and electronic sources, it may be preferable to ask for the request in writing. A written request allows for more clarity about the information to which access is sought, and it provides a record of the request on file.

6.3 A person acting on behalf of the individual

In some situations, a person acting on behalf of the individual may make a request for access. For example, a guardian of the individual may seek access if they have the appropriate legal authority to do so.

For information on circumstances where a parent wants to see their child's health information – see Section 2.9, *Disclosure of health information to a responsible person.*

6.4 Processing a request for access

A useful precaution before processing any request for access is to check the identity of the person making the request, to ensure information is not mistakenly disclosed.

A recommended approach for handling an access request is to:

- Acknowledge the request. When a written request is received, the Privacy Commissioner considers that, ordinarily, it would be reasonable for the individual to expect an acknowledgment within 14 days. The acknowledgement should include an indication of any costs involved in processing the request. (For more guidance, see Section 6.6, *Charging for access.)*

- Where relevant, collate the information requested from the necessary sources. For example, some of the relevant information may be stored electronically and some in paper form.
- Assess the information to make sure there are no details that should be withheld due to any of the provisions under NPP 6.1 or 6.2 (discussed in more detail below).
- Delete or remove any information to be withheld, from any copy or extract of the document being made available.
- Once the information is prepared and cleared for access, provide the information to the individual in the most appropriate form. This should take into account the wishes of the individual. Where access to some information is withheld, it is a legal requirement that the reasons for this decision be provided to the individual.

As a guide, the Privacy Commissioner recommends that the total time for processing a request for access should be no more than 30 days. In some situations, for example where records are held electronically and are simple to process, the time to deal with a request may be significantly shorter.

6.5 Other considerations when providing access

Some factors a health service provider may wish to consider when deciding how best to give access to information could include an individual's disability (if any), or their age or language skills. These factors should not present a barrier to an individual seeking access to their record.

For further guidance on this topic see *Information Sheet 4 – 2001 Access*.

6.6 Charging for access

NPP 6.4

An individual must not be charged for lodging a request for access.

However, individuals may be charged for the administrative costs involved when access is provided. For example, it may be considered reasonable to recover costs relating to photocopying, copies of x-ray films and for staff time involved in processing a request.

If health service providers do charge for providing access, charges must not be excessive and should not discourage an individual from accessing their records.

Tips for compliance

Health service providers are encouraged to bear in mind an individual's circumstances and capacity to pay for access when considering what charges may apply.

When deciding what charges could reasonably apply to requests for access, a health service provider may wish to consult the types of charges that apply in similar access regimes, such as under Freedom of Information laws or under the *ACT Health Records (Privacy and Access) Act 1997*.

6.7 Information withheld in some situations

NPP 6.1

There are a limited number of situations when a request for access may be denied.

In practice, it is likely that information will only need to be withheld on some occasions. On balance, if a situation arises where the individual's right of access weighs equally with the health service provider's concerns about providing access, the Privacy Commissioner encourages providers to err in favour of providing the individual with the information.

Where there is a legitimate reason to withhold access, it is important to keep in mind that this may only apply to part of the health information on the record; access will still need to be provided to the rest of the information.

Access would pose a serious threat to the life or health of any individual

NPP 6.1(b)

There may be cases where a health service provider believes that providing information could present a serious threat to the life or health of the individual or another person. In such cases access may be denied.

A 'serious threat to the life or health of any individual' may include harm to physical or mental health.

The threat must be significant; for example where there is a serious risk an individual may cause deliberate self-harm or where they may harm others. This may include situations where the health service provider believes the information may cause the individual significant distress that may in turn present a serious risk to the individual's health.

Where the health service provider judges that there is a serious threat, and it is possible to provide the information in another form which would remove this threat (for example, by discussing the information in person), then this option could be offered.

Privacy of others may be affected

NPP 6.1(c)

If an individual's record contains information about another person, that information should not be released if it would have an unreasonable impact on the privacy of that other person.

In such situations, to prevent an unreasonable impact on the privacy of other person(s) whose information is on a record, it is suggested that the health service provider take steps such as:

- removing the other person's identifying details before releasing the information. If this approach is taken, care is needed to ensure the remaining context does not reveal the identity of that person;

- contacting the other person to see if they consent to the release of their information. Before taking this approach, a provider should consider whether this action may cause privacy risks for the individual seeking access.

There are situations where releasing information about other person(s) is likely to be less sensitive. These include, for example, where both the individual seeking access and the other person were present at the time the information was collected. Or, if the individual had provided the information about the third party in the first place, there is unlikely to be a concern in giving the individual access to that information.

The request is frivolous or vexatious

NPP 6.1(d)

Information may be withheld where the request is considered frivolous or vexatious. Examples might include where an individual makes repeated requests for information the health service provider has already released or where the request is trivial and made for amusement's sake.

Tip for compliance

Usually, a request for access would not be frivolous or vexatious just because it is an irritation. Health service providers are encouraged to take a careful approach to this provision.

Information relates to existing or anticipated legal proceedings

NPP 6.1(e)

Where there are legal proceedings under way, or where it is anticipated that the health information relates to matters likely to be the subject of future legal proceedings, a health service provider may withhold information that would not be discoverable in those proceedings.

Access would prejudice negotiations with the individual

NPP 6.1(f)

If there are negotiations under way between the health service provider and the individual, for example regarding the settlement of a negligence claim, the provider is not required to release information that may reveal their intentions, and so prejudice the negotiations.

Access would be unlawful

NPP 6.1(g)

A health service provider must not provide access to information where Commonwealth, State or Territory laws expressly prohibit this, or where providing access would breach other statutory or common law.

Denying access is required or authorised by or under law

NPP 6.1 (h)

Access must be denied where the law requires this. Access may be denied where this is authorised by law.

Required by law means that a health service provider must refuse access – they have no choice about this. Authorised by law means that the provider is authorised to refuse access, but has discretion in such circumstances. 'Law' here, applies to State, Territory and Commonwealth laws.

Law enforcement and national security

NPP 6.1(i) (j) and (k)

In any situation where law enforcement or national security authorities may have an interest in the information requested by the individual, a health service provider should consult the provisions in NPP 6 to determine if there is any reason the information may need to be withheld.

Commercially sensitive evaluative information

NPP 6.2

This provision allows a health service provider not to release information that will reveal the formulae, or fine details, of the evaluative process the provider uses in its commercially sensitive business decisions.

In these situations, the health service provider will not need to provide direct access to evaluative information, but will need to explain their decision to the individual.

> *For example, a private nursing home's process for assessing prospective residents may involve recording commercially sensitive information on an individual's record. The nursing home may choose to withhold information that reveals the financial calculations undertaken in reaching its decision. The nursing home will still need to provide access to the raw facts and*

opinions that were input into their evaluative process and a general explanation to the individual about how the decision was reached.

This provision applies in very limited circumstances, and should therefore be applied with care.

For further guidance on this topic see *Information Sheet 4 – 2001 Access and Correction*.

6.8 Use of an intermediary

NPP 6.3

Where a health service provider decides to withhold information from the individual it must, where reasonable, consider whether to use an intermediary. This step will only apply where a decision has been made to refuse access under one or more of the exceptions in NPP 6.1(a) to (k), discussed above.

The role of an intermediary is not to provide an avenue for the access decision to be reviewed. Rather, an intermediary's role is to operate as a facilitator between the individual and the health service provider with the aim of providing sufficient access to meet the needs of both the individual and the provider.

The intermediary must be a person acceptable to both the health service provider and the individual. In the health environment, an intermediary should ideally be another qualified health service provider who both the individual and the original provider believe is suitable to take on the role.

The information to which access has been requested will need to be disclosed to the intermediary (under authority of the individual). This is to allow the intermediary to undertake their role in explaining the contents of that information to the individual. The intermediary must not reveal any specific information or details of information withheld, unless the health service provider decides this is appropriate.

When a health service provider asks an individual whether they would like to use an intermediary, it should be made clear to the individual what will be involved in the process and the extent to which the individual's health information will be disclosed to the intermediary.

Tip for compliance

A health service provider may wish to obtain the individual's written authority before disclosing personal information to the intermediary.

The Privacy Commissioner suggests that the health service provider bear the costs of using an intermediary. However, if the provider is to seek a contribution, or cost-recovery from the individual, they should be advised of the amount involved and agree to the cost obtained before proceeding.

For further guidance on this topic see *Information Sheet 5 – 2001 Access and the Use of Intermediaries.*

6.9 What to tell the individual if information is withheld

NPP 6.7

If information is withheld, the individual must be given reasons for the denial of access.

The health service provider should tell the individual which provision (under NPP 6.1) is being relied upon to refuse access and give reasons accordingly, unless such a disclosure would prejudice an investigation against fraud or other unlawful activity.

6.10 Amendments to individual's health information

NPP 6.5 and NPP 6.6

If an individual believes that personal information about them is not up-to-date, accurate and complete they can ask to have it amended. A health service provider must then take reasonable steps to correct the information.

Where an individual makes a straightforward request, for example to change their name or address, a health service provider could make these changes via usual processes provided they are satisfied of the identity of the individual.

More complex issues arise when an individual challenges an opinion, evaluation or diagnosis that is in their health record, and seeks to have this corrected.

There may be important medical and legal reasons for retaining a complete record. Therefore, if an individual asks to have certain details amended or corrected, the health service provider should generally attach comments to the record noting the correct information rather than permanently erasing details from the health record.

Where the individual and the health service provider disagree about whether the information is incorrect, the provider must take reasonable steps to attach to the information a statement outlining the individual's claims that the information is not accurate, up-to-date or complete.

There may be situations when an individual will feel strongly that they do not want certain health information, which is agreed to be incorrect and misleading, to remain on the medical record. An example of this might be where an agreed incorrect diagnosis of a psychiatric condition has been noted on the record.

If, in exceptional circumstances, a health service provider decides that there are greater risks in leaving certain information on the record than in erasing it,

erasure or deletion of the relevant part of the health record may be appropriate. However, this should not be done without fully considering potential legal or medical implications. It is expected that permanently erasing information from an individual's record would only be justified in rare circumstances.

7 Identifiers

National Privacy Principle 7

This principle sets out a health service provider's obligations when handling Commonwealth identifiers. It prohibits the adoption of Commonwealth identifiers, by health service providers, except in prescribed circumstances.

This principle also prohibits the use or disclosure of Commonwealth identifiers except where these uses or disclosures are necessary to fulfil obligations to Commonwealth agencies; or where certain other provisions apply.

The use of identifiers can contribute to handling records efficiently, matching data with confidence, and storing and accessing records in a structured manner.

However, there are some inherent privacy risks. For example, identifiers can allow large quantities of data about an individual, from different sources, to be brought together on a single database. This may make it more difficult for the individual to control how information about them is handled.

This principle is intended to control the use and disclosure of Commonwealth-assigned identifiers. The principle does not apply to identifiers issued by State or Territory government agencies (such as driving licence numbers). Nor does the principle cover identifiers created by individual health service providers. There are, however, relevant state laws that apply to some State-issued identifiers.

7.1 What is an identifier?

In the Privacy Act, an 'identifier' is defined as:

> a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations

An identifier can be numbers, letters or both, but is not limited to letters or numbers. An individual's name is not an identifier.

The principle only applies to the adoption, use and disclosure of identifiers that have been issued by Commonwealth Government agencies. For example, the:

- Medicare number; and
- Department of Veterans' Affairs number.

7.2 Limitations to the use of identifiers

The principle places limits on how an identifier may be handled by other organisations, including health service providers.

One of the key requirements of this principle is that health service providers must not adopt as an identifier of an individual, for its own purposes, any identifier already assigned by, or on behalf of, a Commonwealth government agency, unless special regulations have been made under s.100 of the Privacy Act. To date no such regulations have been made.

This means that such identifiers must not be used as the basis for a health service provider's own identification system.

> For example, a health service provider could not adopt the Medicare number as their own identifier.

A health service provider may only use, disclose or keep a record of these identifiers:

- where necessary to meet any obligations to the relevant agency;
- in accordance with NPP2.1(e), (f), (g) or (h), if they apply (Chapter 2, *Use and Disclosure*, gives more information on these provisions); or
- where these activities occur for 'prescribed' circumstances relating to a regulation made subject to s.100 of the Privacy Act.

> Therefore, it is acceptable to use a Medicare number to determine an individual's eligibility to receive health services funded under Medicare.

8 Anonymity

National Privacy Principle 8

This principle sets out a health service provider's obligation to make available to individuals the option of not identifying themselves when entering transactions with the provider, wherever this is lawful and practicable.

8.1 Using a health service anonymously

In a number of situations an individual may wish to remain anonymous or use an alias when seeking health care. In some cases, an individual may be hesitant to seek health care or treatment unless they know that they will be able to do so without revealing their identity. Individuals do not have to state a reason to request anonymity.

Situations where people may not wish to identify themselves include:

- using counselling services, including phone counselling, on sensitive issues such as drug use, suicide or gambling addiction;
- attending sexual health clinics for health advice;
- using a health service where the individual fears for their safety. For example, in relation to counselling for domestic violence where the individual may fear retaliation from their partner; or
- using services in a small community where friends or colleagues may have access to information on the health system. This can also be an issue for staff of health service providers who have had to attend that provider's service in a personal capacity.

The use of an alias may also be appropriate for cultural reasons, such as with members of the indigenous community who may require aliases in certain circumstances. (For further information see the Privacy Commissioner's publication *Minding Our Own Business – Privacy Guidelines for Aboriginal and Torres Strait Islander People*.)

8.2 Anonymous service which is not lawful

In some situations it may not be lawful to provide a service anonymously.

Generally, this is because there is a legal requirement for the health service provider to collect identifying information from the individual.

> For example, some State and Territory public health laws require providers to collect identifying information regarding individuals diagnosed with certain notifiable diseases.

Also, individuals often need to provide identifying information in order to have prescriptions written and filled.

8.3 Anonymous service which is not practical

There will be situations where it is not practicable to give an individual the option of using a health service anonymously. Factors that affect practicability may include:

- whether anonymity would jeopardise the quality and timeliness of the health care provided;
- whether identification is required to provide a health service;
- the cost of providing services anonymously; and
- medico-legal factors.

For example, in some situations it may be difficult to provide adequate health care to an individual if their use of services cannot be accurately monitored. This may be the case in a hospital where the treating team needs to share information about the individual, and where follow-up is important.

Tips for compliance

Health service providers could consider providing for the use of aliases within a particular health service as a means of providing a degree of anonymity.

Any new systems or practices developed should, where practicable and lawful, allow individuals to use the service without having to be identified.

9 Transborder data flows

National Privacy Principle 9

This principle sets out a health service provider's obligations when transferring personal information outside Australia. These include only transferring data overseas where:

- there is a reasonable belief the recipient is subject to a comparable information privacy scheme; or
- the individual has given consent; or
- the transfer of data is necessary to the performance or completion of a contract requested by, or in the interest of, the individual; or
- the transfer is for the benefit of the individual, it is impracticable to obtain consent and the provider can show grounds for a belief that if it were practicable to obtain consent, the individual would be likely to give it; or
- other reasonable steps have been taken to ensure that the information will be held, used or disclosed consistently with the NPPs.

A health service provider will need to take these obligations into account if asked to provide a medical report to an organisation in another country (for example, to a foreign immigration agency or to a health service provider in a country the individual is visiting).

This principle also applies if, for example, health information is requested for research purposes by an overseas organisation.

As a general rule, if a health service provider has the individual's consent to transfer their health information overseas, then this can occur. Otherwise, the provider must consider the other requirements set out under this principle, when determining whether information may be transferred.

The principle does not prevent transfers of personal information outside Australia by a health service provider organisation to another part of the same organisation (such as a branch in another country), or directly to the individual concerned. Note that the application of this principle depends on the details of the relevant corporate structure.

> For example, some overseas transfers of personal information may be between an Australian subsidiary and the overseas parent company. Those within the companies may consider them to be different parts of the same organisation, when sometimes they are separate legal entities, in which case transfers may only occur if one of the provisions in NPP 9 applies.

Given that transferring personal information overseas may remove it from the protection of Australian law, a health service provider relying on NPP 9(a) or NPP 9(f) may need to be in a position to give evidence about the basis on

which it decided it met the requirement of 'reasonable belief' or 'reasonable steps'.

Tips for compliance

Getting a legal opinion would be a good way for a health service provider to get evidence about its basis for deciding it has met the 'reasonable belief' or 'reasonable steps' requirements in NPP 9, before transferring information overseas.

To give properly informed consent to the transfer of their information overseas, individuals should generally be aware of the applicable privacy regime in the country to which the information is to be sent, and the impact this will have on the individuals' existing privacy rights.

10 Change in business circumstances or closure of a health service

NPP 2, NPP 4, NPP 6 and NPP 10

This chapter considers the privacy implications of changes in the business circumstances of health service providers, including the cessation of business.

A health service provider's business circumstances could change in a number of ways. A provider may amalgamate with other providers or businesses, another business may take over the existing provider's practice, the provider may close down, or the services may cease because the health service provider (if they are a sole practitioner) retires or dies.

Taken together, the NPPs place requirements on health service providers facing any of these changes.

10.1 Information stays with the original health service provider organisation

In some cases, the nature or ownership of a health service provider changes, but the legal entity or organisation remains in existence. Here, the NPPs do not require any additional action unless the organisation is proposing to change the purposes for which it uses or discloses personal information. The new purposes would need to be addressed in ways consistent with the provisions of NPP 2.

If the health service provider uses an individual's health information as it did before, in providing health care, then there is no requirement to inform, or seek consent from, the individual.

However, if as a result of the change, the health service provider intends to use the information for purposes that are not consistent with the primary purpose of collection, or are not directly related secondary purposes and within the reasonable expectations of the individual, then the provider may need to seek consent.

> For example, a general practice expands, creating a medical centre with same-provider pathology, radiology, counselling and other services.
>
> The provider wants all patient health information to be available to all their health professionals, some of whose services have no direct relation to the reasons the individual consults the general practitioner. As some of these uses may fall outside the individual's reasonable expectations, NPP 2 may require that consent be sought, unless one of the exceptions to the principle applies.

10.2 Information is moved to a new health service provider

In circumstances where there is a new legal entity, for example in some takeovers or mergers, there may be a transfer of personal information. Under the NPPs this means there will be a disclosure by the old organisation and collection and use by the new organisation. The relevant information handling standards here are NPP 2 (for use and disclosure) and NPPs 1 and 10 (for collection).

> For example, when a health service provider closes, selling their operations to a wholly new provider, the new provider will take over their assets and patient-base (including databases).

Disclosure by the old health service provider

The NPPs permit disclosure of health information without further obligations where this is for the primary purpose for which the information was collected, or where the disclosure is directly related to the primary purpose and within the individual's reasonable expectations.

If the old health service provider is satisfied that a new or resulting entity will continue to provide essentially the same service, in very similar circumstances, it could proceed with disclosure on the grounds that it is consistent with the primary purpose.

If the new organisation proposes something different, the old health service provider will then need to consider if the proposed uses are directly related and what individuals might expect (under NPP 2.1(a)). If the old provider is satisfied that the disclosure is related and within reasonable expectations, again it may proceed.

Where there is doubt about whether disclosures would be consistent with the approaches mentioned above, the safer course would be to obtain consent before disclosing health information.

Collection and use by the new organisation

Ordinarily, the new health service provider will need consent before collecting individuals' health information, unless one of the exceptions to NPP10 applies. The provider may also need to tell the individuals that it now holds information about them, give its contact details and other information (as required by NPP1.3 and NPP1.5). These obligations are detailed in Chapter 1, *Collecting Health Information*.

The old and the new health service providers may decide between them how to handle these obligations.

If an individual does not consent to the transfer of their information, they may wish to have it transferred to another health service provider. This is further discussed in Chapter 2, *Use and Disclosure*.

10.3 A health service provider's business ceases

Where a health service provider ceases operations and no other provider is taking over, arrangements will need to be made for the appropriate storage and transfer of individuals' health information. This situation might occur where a health service provider retires or dies.

Generally, the destruction of health information in this circumstance is not good practice. Destruction may also be inconsistent with other laws or regulations.

In the event that the health information is to be transferred to another health service provider, then consent for disclosure and collection may need to be obtained (see the discussion above).

Where individuals cannot be contacted, appropriate arrangements may need to be made to secure the data for future access by those individuals, or for other permitted uses and disclosures.

See Chapter 4, *Data Security,* for more information on NPP4 requirements regarding secure storage and appropriate destruction of health records.

Tip for compliance

It is good privacy practice for a health service provider to notify individuals of the closure or cessation of service, when it is practicable to do so.

Appendix 1 – National Privacy Principles

Extracted from the Privacy Act 1988

Schedule 3—National Privacy Principles

Note: See section 6.

1 Collection

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 An organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or, if that is not practicable, as soon as practicable after) an organisation collects personal information about an individual from the individual, the organisation must take reasonable steps to ensure that the individual is aware of:

(a) the identity of the organisation and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) the organisations (or the types of organisations) to which the organisation usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.

1.5 If an organisation collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in subclause 1.3 except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual.

2 Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless:

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection;

(ii) the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) it is impracticable for the organisation to seek the individual's consent before that particular use; and

(ii) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(iii) the individual has not made a request to the organisation not to receive direct marketing communications; and

(iv) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(v) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be directly contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph; and

(iii) in the case of disclosure—the organisation reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(f) the organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the organisation reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter organisations from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires an organisation to disclose personal information; an organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: An organisation is also subject to the requirements of National Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If an organisation uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, an organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual if:

(a) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the ***carer***) providing the health service for the organisation is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is ***responsible*** for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

(c) a spouse or de facto spouse of the individual; or

(d) a relative of the individual, at least 18 years old and a member of the individual's household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

(g) a person who has an intimate personal relationship with the individual; or

(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child of an individual includes an adopted child, a step-child and a foster-child, of the individual.

parent of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3 Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4 Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

5 Openness

5.1 An organisation must set out in a document clearly expressed policies on its management of personal information. The organisation must make the document available to anyone who asks for it.

5.2 On request by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

6 Access and correction

6.1 If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or

(c) providing access would have an unreasonable impact upon the privacy of other individuals; or

(d) the request for access is frivolous or vexatious; or

(e) the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

(f) providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: An organisation breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the organisation must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If an organisation charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so.

6.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

7.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency; or

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2).

7.2 An organisation must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency; or

(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2).

7.3 In this clause:

identifier includes a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an ***identifier***.

8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

9 Transborder data flows

An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:

(a) the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the NPPs; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the NPPs.

10 Sensitive information

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) if the information is collected in the course of the activities of a non-profit organisation—the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities;

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

10.3 Despite subclause 10.1, an organisation may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) it is impracticable for the organisation to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law (other than this Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation; or

(iii) in accordance with guidelines approved by the Commissioner under section 95A for the purposes of this subparagraph.

10.4 If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to permanently de-identify the information before the organisation discloses it.

10.5 In this clause:

non-profit organisation means a non-profit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

Appendix 2 – Definitions from the Privacy Act (1988)

Health information means:

(a) information or an opinion about:

(i) the health or a disability (at any time) of an individual; or

(ii) an individual's expressed wishes about the future provision of health services to him or her; or

(iii) a health service provided, or to be provided, to an individual;

that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances.

Health service means:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:

(i) to assess, record, maintain or improve the individual's health; or

(ii) to diagnose the individual's illness or disability; or

(iii) to treat the individual's illness or disability or suspected illness or disability; or

(b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

The term **health service provider** as used in these Guidelines means a provider of a health service. The term 'health service provider' is not separately defined in the Privacy Act.

Personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Sensitive information means:

(a) information or an opinion about an individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) membership of a professional or trade association; or

(vii) membership of a trade union; or

(viii) sexual preferences or practices; or

(ix) criminal record;

that is also personal information; or

(b) health information about an individual.