



Divisions of General Practice

Information Management Maturity Framework
(IMMF)

**Toolkit – Privacy guidelines for
reuse of information**

Information Management Maturity Framework Toolkit – Privacy guidelines for reuse of information

Purpose

The purpose of the “ Privacy guidelines and checklist” is to assist Divisions to address the action tasks below.

Action Tasks	Capacity Task	Element of IM
Implement a common security and privacy standard for all of the Division’s programs and services	Reactive to Defined	Compliance and Quality

This task should have been identified from the IMMF gap analysis and toolkit specification.

This tool provides the CEO with a simple explanation of what is required by a Division to meet the legislative requirements and obligations in relation to Commonwealth Privacy Act (1988) to personal information used within the Division. Examples of good practice and practical lessons learned from Divisions of General Practice are documented for discussion.

The knowledge of and application of the Privacy Act, and its associated principles are fundamental to the collection, storage and use of **any** personal information by the Division.

Application of the Privacy Act and its principles cuts across all areas of Information Management, and underpins the use of any personal information by the Division.

Explanatory notes

The Commonwealth Privacy Act (1988), requires the Division to enact practices, policies and procedures, which support the protection of personal information. This includes all personal information that has, or will be collected, held or shared by the Division in any form. CEOs also need to be familiar with the Privacy Act for their own State or Territory. In general, though, State and Territory laws are consistent in with Commonwealth Act. Where there is a variation between provisions of the Commonwealth and other jurisdictions, the Division should comply to the most rigorous legislation. In most cases this is the Commonwealth Act.

The development of common awareness and understanding of the Act and its principles, by all staff, will enable the Division to consistently meet its obligation and responsibilities as defined in the Act.

The information used within this guide has been derived from the Privacy Commissioner and application of the act within Divisions of General Practice

Instructional Design

This tool consists of two parts;

Part 1- Privacy Act and Protection of Personal Information.

Part 2 – Privacy Checklist

Part 1 – Privacy Act and Protection of Personal Information.

The CEO should review the ten Privacy Principles contained within the Privacy Act (1988). Starting with the senior staff, all staff are to be trained either in small groups or all at once, on privacy principles and how to apply them to situations faced within the Division.

Qualified State Based Organisation staff may be available to assist and to provide advice on processes that other Divisions have used manage privacy issues activities. CEOs will find value in discussing their experiences and requirements with executive staff at other Divisions that have demonstrated a capacity to appropriately introduce and develop polices procedures and practices consistent with the Act.

There is a wide range of material available on application of privacy principles for Health Organisations from the Office of Privacy Commissioner, including clinical examples, policy examples and Frequently asked questions (FAQs).

After the review, the CEO should be able to identify gaps in staff knowledge of and application of the Privacy Act and Privacy Principles; or in processes or procedures to support the application of the Act; or the needs that require addressing through training and or ongoing review.

Part 2 - Privacy Checklist

CEOs and their senior program staff should review the Privacy Principles and checklists. Information may be available from State Based Organisations to assist in the review and to provide advice on how to start and begin incorporating privacy principles into existing policies and procedures.

CEOs should discuss the successful implementation of Privacy Principles, associated policies and procedures with senior staff at other Divisions that have identified activities or processes that have successfully applied and incorporated Privacy Act into their Division.

After the review, CEOs should identify objectives for their Division for improvement of the application of the Privacy Principles and ongoing adherence to the Privacy Act.

Workstreams	Outcomes	Resources
Skills or knowledge acquisition requirements for staff.	Senior program staff are aware of the Privacy Principles and can apply them to practical situations within the Division. All staff are aware of privacy principles and their application to personal information.	Mentoring by CEOs of Divisions that have demonstrated a capacity for implementation of Privacy Principles. Group workshops will be held to provide training about and application of Privacy Act and Privacy Principles.
New policies and / or procedures to be adopted.	Policies and / or procedures are developed to identify and manage personal information within Division.	State based office staff may also be available for facilitation and support for new policies and / or procedures Materials available from Privacy Commissioner.
Culture and change management requirements.	There is active support for Privacy Principles from most staff. A framework exists for individuals and teams to incorporate Privacy Principles into the Division practices.	Mentoring by CEOs of Divisions that have demonstrated a capacity for implementation of privacy principles.

Part 1 – Privacy Act and Protection of Personal Information.

Many Divisions already have sophisticated processes and procedures for incorporating the Privacy Act and its principles into their day to work within the Division. The information provided in this tool is designed to raise awareness and enhance the application of Privacy Principles within all Divisions.

Within a particular Division the capacity to implement the Privacy Act and its principles relies on two factors;

- Understanding the Legislation and applying it to practical examples within the Division; and
- Managing the Acts application process within the Division to ensure sustainable outcome.

The key to successful adoption of new ways of working within a Division is engagement, consultation and education.

Who must comply with Privacy Act (1988) ?

All health service providers in the private sector, and those who work as contractors to the Commonwealth. Consequently, all Divisions and their staff, must comply with the Commonwealth Privacy Act (1988), and the associated ten National Privacy Principles when handling personal information.

Ten Privacy Principles

The Privacy Act has ten privacy principles in relation to information. These are;

- Collection
- Use and Disclosure
- Data Quality
- Data Security
- Openness
- Access and Correction
- Identifiers
- Anonymity
- Transborder data flows
- Sensitive Information

Application of Commonwealth Privacy Principles;

The Commonwealth privacy Commissioner has provided advice of how each of the ten National Privacy Principles ('NPPs') relate to the collection and use of these are patient information by Private Health Sector. (See Appendix 1 for a full description of the National Privacy Principles).

NPP1: Collection & NPP10: Sensitive Information – set out providers' obligations when collecting health information from patients. These include collecting health information only with consent, and collecting only the information necessary to provide the service.

NPP2: Use and Disclosure – set out how health information, once collected, can be used within the organisation or disclosed to third parties outside the organisation.

NPP3: Data Quality & NPP4: Data Security – set standards for keeping information up-to-date, accurate and complete, as well as for protecting and securing it from loss, misuse and unauthorised access.

NPP5: Openness – requires providers to be open about how they handle health information, including the need to develop a document (such as a privacy policy) to clearly explain how they handle health information.

NPP6: Access & Correction – gives patients a general right of access to their own health records, and a right to have information corrected, if it is inaccurate, incomplete or out of date.

NPP7: Identifiers – limits the use of Commonwealth Government identifiers (such as the Medicare number or the Veterans Affairs number) by providers to the purposes for which they were issued.

NPP8: **Anonymity** - where lawful and practicable, patients must have the option of using health services without identifying themselves.

NPP9: **Transborder data flows** – sets out obligations for providers regarding the transfer of health information out of Australia.

(New Privacy Law & the Private Health Sector, 2001; Office Privacy Commissioner)

Commonwealth and State Legislation;

Where a State law is inconsistent with a Commonwealth law, the Commonwealth law will apply. Consequently, all private sector health service providers are required to comply with the Commonwealth Privacy Act (1988) unless employed in a State Department where they are covered by the relevant State and Territory Privacy Acts. In general, though, State and Territory laws are consistent in with Commonwealth Act. Where there is a variation between provisions of the Commonwealth and other jurisdictions, the Division should comply to the most rigorous legislation. In most cases this is the Commonwealth Act.

Collection of Information for Business or Management Purposes;

The Commonwealth Privacy Act (1988) does identify where personal information may be used for other purposes, such as managing the business e.g. audits of clinical files or overview of a clinical program to ensure safety and efficacy. However the personal information used for this purpose, must be consistent with the primary purpose of collection (for example, it was originally collected as part of a medical treatment). However, if the personal information is sensitive information, as defined in the act. It's reuse must directly relate to the primary purpose for which it was collected, and cannot be used for other purposes without the persons consent. (See Glossary).

Importantly the use any personal information must be consistent with what the individual would reasonably expect the organisation to use or disclose the information such as operating a safe and secure service.

As a matter of course and best practice, it is better to inform all people who use the service and provide personal information as to why it is being collected, and how it is to be used.

De-identified Data

Privacy Acts only apply to identified data, so using de-identified data proves less of an issue. However it is important to ensure that the process of de-identification cannot be reversed. This is done by permanently removing identifiers. If only names have been removed from data sets they are still potentially identifiable.

The National Health and Medical Research Council (NHMRC) has highlighted that the process of de-identification can be irreversible if the identifiers have been removed permanently or the data have never been identified. These data are referred to as "de-identified". It should be recognised that the term "de-identified" is used frequently, in documents other than this Statement, to refer to sets of data from which only names have been removed. Such data may remain "potentially identifiable."
<http://www.nhmrc.gov.au/publications/humans/appndix3.htm>

Commercial in Confidence:

It is also important for Divisions to understand that general practice can sometimes have a commercial interest in the data a practice may hold and, in addition to the personal privacy requirements it is important for Divisions to respect this interest and seek the permission of the practice before it is used.

Research;

The Division must gain consent from any participant of *research* project or study where personal or identifiable information is collected or used. As a matter of good practice, any proposed research that uses identifiable or private information should seek ethical approval from appropriate State or Territory authority.

When using health data for research it is essential to gain re-consent for every new research project. GPs cannot get patients to sign blanket consent forms to cover the use of their identified health information in new research projects. They have to gain consent for each individual project.

Safety and Security;

All personal information on a record (See Glossary) in any form, that is electronic or in hard form; paper must be stored safely and securely. A Division must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure. In general, the more sensitive the personal information and the more readily it can be used to identify an individual or group the more secure its storage and management must be.

Free Privacy Act and principle guides, handbooks and templates can be found from many online resources. Some that have been reviewed as suitable for use by Divisions are:

The Australian Privacy Commissioner; Excellent resource and the best starting point for information;

<http://www.privacy.gov.au/>

List of State and Territory laws; compiled by the Australian Privacy Commissioner;

http://www.privacy.gov.au/privacy_rights/laws/index.html - 1

Health issues and fact sheets; compiled by the Australian Privacy Commissioner;

<http://www.privacy.gov.au/health/index.html>

The General Practice Computing Group (GPCG); Produced a useful range of resources in relation to privacy and security and a range of links to other resources.

http://www.gpcg.org.au/index.php?option=com_content&task=view&id=75&Itemid=107

The Royal Australian College of General Practitioners (RACGP) ; Has an excellent range of resources on privacy within the practice support section of there web site.

<http://www.racgp.org.au/privacy>

Monash Division of General Practice; has a series resources it has produces.

National Health and Medical Research Centre, has information on de-identified data.

<http://www.nhmrc.gov.au/publications/humans/appndix3.htm>

<http://www.monashDivision.com.au/resources/resources.htm>

The Alliance of NSW Divisions; has a series of checklists and resources.

<http://www.answd.com.au/intro.asp>

Part 2 - Privacy Checklist

The headings and notes below are a checklist of the topics to be considered during the awareness raising and application of privacy principles within Division..

- Are you aware that the Division must operate under the Commonwealth Privacy Act (1988) ?
- Have you read the ten National Privacy Principles? (See Appendix 1)
- Have you made all staff within the Division aware the Act and the ten National Privacy Principles? If not how do you intend to ?
- Are you aware of the definition of 'sensitive information'? Does the Division collect sensitive information?
- Does the Division share or collect information with external organisations or groups ? If yes, is the Division aware of its responsibilities when doing so ?
- Do you understand the concepts of 'primary purpose', 'secondary' purpose' and 'reasonable expectations' in relation the collection, use and disclosure of personal information held and collected by the Division?
- Are you confident your staff are familiar with the privacy legislation and their individual responsibilities under it within the practice?
- Have you conducted a privacy audit of your Division's current practices and procedures?
- Have you conducted a security review of your Division's current practices and procedures?
- Have you formulated or adopted a privacy policy? If so has this been presented to the Division's Board for ratification or endorsement?
- Have you trained your staff in relation to the Division's privacy policy and procedures?
- Do staff make all people who provide personal information to the Division aware of their rights and responsibilities under the privacy Act?
- Has the Division developed a policy about handling requests for access and amend to records by people who have provided personal information?
- Has the Division developed a procedure to handle complaints or incidents regarding breaches of privacy?
- Have you initiated an ongoing review process to determine the Division's adherence to its privacy policy and procedures, and its compliance with privacy legislation?
- Have you considered appointing a Privacy Officer?

(Adapted from; Privacy Resource Handbook For all Medical Practitioners in the Private Sector, 2002)

Glossary

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; or
- (d) genetic information about an individual in a form that is, or could be, predictive of the health of the individual or a genetic relative of the individual.

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.

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.

A record means:

- (a) a document; or
- (b) a database (however kept); or
- (c) a photograph or other pictorial representation of a person;

A record does not include:

- (d) a generally available publication; or
- (e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or
- (f) Commonwealth records as defined by subsection 3(1) of the *Archives Act 1983* that are in the open access period for the purposes of that Act; or

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; or
- (c) genetic information about an individual that is not otherwise health information.

End of Document

Appendix 1

Schedule 3—National Privacy Principles

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
- (ea) if the information is genetic information and the organisation has obtained the genetic information in the course of providing a health service to the individual:
 - (i) the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety (whether or not the threat is imminent) of an individual who is a genetic relative of the individual to whom the genetic information relates; and
 - (ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under section 95AA for the purposes of this subparagraph; and
 - (iii) in the case of disclosure—the recipient of the genetic information is a genetic relative of the individual; 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 subsections 100(2) and (3).

- 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 National Privacy Principles; 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 National Privacy Principles.

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 or authorised by or under 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.