




Divisions of General Practice

Information Management Maturity Framework
(IMMF)

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



Information Management Maturity Framework (IMMF)

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 Gap | IMMF Element |
|--|---------------------|------------------------|
| 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 Information Management Maturity Framework (IMMF) gap analysis and toolkit specification.

This tool provides the Chief Executive Officer (CEO) with a simple explanation of what is required by a Division to meet the legislative requirements and obligations set out by the Privacy Act 1988 (Commonwealth) – including later amendments that apply to the private sector. Examples of privacy scenarios and practical lessons learned from Divisions of General Practice are documented for discussion.

Knowledge of and application of the Privacy Act and its associated principles is fundamental to the collection, storage and use of all personal information handled by the Division. The Privacy Act and its principles cut across all areas of information management (IM) and underpin the use of any personal information by the Division.

While all care has been taken in the development of this toolkit, privacy is a complex area. Therefore it is important to read the disclaimer provided by the Commonwealth Department of Health and Ageing which immediately follows the reference section of this toolkit.

Explanatory notes

The Privacy Act requires any Division of General Practice to enact practices, policies and procedures which support the protection of personal information. This includes all personal information that is handled and / or shared by the Division in any form, regardless of how it comes to be held by the Division.

CEOs also need to be familiar with applicable privacy legislation for their own State or Territory, as well as certain legislation in some places specific to health information. In most respects, State and Territory laws are not dissimilar to the Commonwealth Privacy Act. However, where there is a variation between provisions of the Commonwealth and other jurisdictions, the Division should seek to comply with the more rigorous legislation.

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

A list of sources and references used to develop this tool is attached at the end of the document.

Instructional design

This tool consists of three Parts:

Part 1 – Privacy Act and Protection of Personal Information

Part 2 – Case studies

Part 3 – Privacy checklist

The tool also includes a glossary and an appendix containing the 10 National Privacy Principles.



Part 1 – Privacy Act and Protection of Personal Information

The CEO should be familiar with the ten National Privacy Principles (NPPs) contained within the Privacy Act 1988 (Commonwealth). Starting with the senior staff, all staff are to be trained on privacy principles and how to apply them to situations faced within the Division. The CEO needs to be able to identify gaps in staff knowledge regarding the Privacy Act and its practical application, including processes and procedures to support implementation of the Act. Significant gaps when identified should be addressed through training and or ongoing review.

Qualified State Based Organisation (SBO) staff may be available to assist and to provide advice on processes that other Divisions have used to manage privacy issues activities. CEOs will find value in discussing their experiences and requirements with executive staff of other Divisions that have demonstrated a capacity to appropriately introduce and develop policies 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 the Privacy Commissioner and other industry sources, including clinical examples, policy examples and frequently asked questions (FAQs). See References below.

Part 2 – Case studies

To assist Divisions in the practical application of the Privacy Legislation and associated principles three case studies are provided. When considering the case studies Divisions should reflect upon how they would deal with similar situations and how their current policies would deal with the identified issues.

Part 2 - Privacy checklist

CEOs and their senior program staff should review the National Privacy Principles and the checklist provided in this toolkit. Information may be available from SBOs 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 reviewing their Division's understanding of the Privacy Act and 10 NPPs, CEOs should identify objectives for their Division for improvement of the application of, and ongoing adherence to the Act.

Summary of outcomes and resources

| Workstreams | Outcomes | Resources |
|--|---|--|
| Skills or knowledge acquisition requirements for staff | <p>Senior program staff are aware of the Privacy Principles and can apply them to practical situations within the Division.</p> <p>All staff are aware of privacy principles and their application to personal information.</p> | <p>Mentoring by CEOs of Divisions that have demonstrated a capacity for implementation of Privacy Principles.</p> <p>Group workshops will be held to provide training about and application of Privacy Act and Privacy Principles.</p> |
| New policies and / or procedures to be adopted | <p>Policies and / or procedures are developed to identify and manage personal information within Division.</p> | <p>State based office staff may also be available for facilitation and support for new policies and / or procedures. Materials available from Privacy Commissioner: see References below.</p> |



| | | |
|---|---|---|
| Culture and change management requirements | <p>There is active support for Privacy Principles from most staff.</p> <p>A shared understanding exists through which individuals and teams can incorporate Privacy Principles into the Division practices.</p> | <p>Mentoring by CEOs of Divisions that have demonstrated a capacity for implementation of privacy principles.</p> |
|---|---|---|



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 day work. The information provided in this tool is designed to raise awareness and enhance the application of Privacy Principles within all Divisions.

Who must comply with Privacy Act 1988 (Commonwealth)?

Given the more recent private sector amendments, the Privacy Act 1988 (Commonwealth) has a very broad scope. The Act applies to all health service providers in the government and private sectors, and those who work as contractors to the Commonwealth. Consequently, all Divisions and their staff must comply with the Act and the 10 National Privacy Principles when handling personal information.

Note that Privacy Principles relating to trans-border data flows impose obligations on the sender of personal information to ensure that recipients apply comparable standards of care over privacy. Certain state privacy legislation in Australia expressly covers trans-border flows between states. Commonwealth privacy legislation generally provides exemptions for small businesses but not if those small businesses handle health information. Divisions must bear this in mind as they exchange health information from time to time with private sector organisations regardless of their size.

The National Privacy Principles in summary

Here are the 10 National Privacy Principles and a brief explanation of the “headline” obligations associated with each of them. (See the Appendix for a full description of the National Privacy Principles).

In summary, the major implications of the 10 NPPs are as follows:

- NPP1: **Collection** – Divisions must only collect personal information for reasons directly related to their business or operational requirements;
- NPP2: **Use and Disclosure** – Divisions must explain how and why personal information can be used within the organisation or disclosed to external third parties under special circumstances;
- NPP3: **Data Quality** – Divisions must take reasonable steps to ensure that personal information is up-to-date, accurate and complete;
- NPP4: **Data Security** – Divisions must take reasonable steps to ensure that personal information is secure from loss, misuse and unauthorised access;
- NPP5: **Openness** – Divisions must be open about how they handle health information and clearly explain how they handle health information;
- NPP6: **Access & Correction** – Patients have a general right of access to their own health records, and a right to have information held by a Division corrected, if it is inaccurate, incomplete or out of date;
- NPP7: **Identifiers** – Divisions must not use Commonwealth Government identifiers (such as Medicare number or Veterans Affairs numbers) to identify patients for their own record keeping purposes. These identifiers may only be used on disclosure for the reasons they are issued;
- NPP8: **Anonymity** – Divisions must, where lawful and practicable, provide patients with the option of using health services without identifying themselves;



NPP9: **Transborder data flows** – Divisions must take care that adequate privacy regimes apply in other jurisdictions – which in some states of Australia means other states – into which they might transfer personal information;

NPP10: **Sensitive Information** – Divisions have additional obligations when collecting health information from patients as this is counted as “sensitive” under the Privacy Act. These include collecting health information only with consent.

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 expressly covered by local legislation. Broadly speaking, State and Territory privacy laws are similar to the Commonwealth Act. Where there is a variation between provisions of the Commonwealth and other jurisdictions, the Division should comply to the most rigorous legislation.

What follows is a brief, and not necessarily complete, overview legislation and regulatory instruments that are relevant to health information at state and federal level, including identification of the various sets of privacy principles that may be applicable to Divisions in different places.

Remember that while a Division might strictly speaking constitute a federal government entity, Divisions routinely interact with local healthcare organisations, in both public and private sectors, and that they can therefore find themselves being touched by state and territory laws.

Commonwealth

The *Privacy Act 1988 (Commonwealth)* and *Privacy Amendment (Private Sector) Act 2000 (Commonwealth)* are the peak pieces of legislation nationally. They apply to all Commonwealth government agencies and most of the private sector. They establish:

- 10 National Privacy Principles (NPPs) that apply in the private sector, and
- 11 Information Privacy Principles (IPPs) that apply to federal and ACT government agencies.

Managed by The Privacy Commissioner: <http://www.privacy.gov.au>

When starting to consider issues of privacy a Division should utilise the extensive range of materials produced by The Privacy Commissioner. The Privacy Commissioner produces a wide range of materials including checklists, briefing documents, Health Issues and Fact Sheets. These are available online at <http://www.privacy.gov.au/health/index.html>.

NSW

Note that the *Privacy and Personal Information Protection Act 1998 (NSW)* excludes health information, which is covered instead by the *Health Records and Information Privacy Act 2002 (NSW)*. This law establishes:

- 15 Health Privacy Principles (HPPs) grouped into seven areas: collection, storage, access and accuracy, use, disclosure, identifiers and anonymity, and transferrals and linkage.

Managed by, Office of the NSW Privacy Commissioner:
http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_index.



Victoria

Victoria has two important pieces of legislation: the *Information Privacy Act 2000 (Vic)* and the *Health Records Act 2001 (Vic)*. Together these establish:

- 10 Information Privacy Principles similar to the NPPs; and
- 11 Health Privacy Principles adapted from the NPPs in the Privacy Act.

Managed by the Office of the Victorian Privacy Commissioner:
<http://www.privacy.vic.gov.au/dir100/priveb.nsf>

Queensland

The state of Queensland as yet as no privacy legislation. Administrative instructions are however in force across state agencies, with details obligations laid down by the Queensland government *Information Standard 42A—Information Privacy for QH* which includes a subset of the 10 NPPs.

This is managed by the Department of Justice and Attorney-General: <http://www.privacy.qld.gov.au/>

Western Australia

The state of Western Australia (WA) has no privacy legislation as yet (as of April, 2008), but the *Information Privacy Bill 2007 (WA)* has been introduced to Parliament. Divisions in WA should note that the draft bill sets out 10 Health Privacy Principles which are broadly similar to the NPPs but are specifically tailored health information.

Managed by the Office of the Information Commissioner: <http://www.foi.wa.gov.au>

South Australia

The state of South Australia (SA) has no privacy legislation as yet (April, 2008), but a *Code of Fair Information Practice* is in force for the SA Department of Health and the SA Department for Families and Communities. The SA Code is based on the NPPs.

Managed by the Privacy Committee: <http://www.archives.sa.gov.au/privacy/committee.html>

Tasmania

The *Personal Information Protection Act 2004 (Tas)* establishes:

- 10 Personal Information Protection Principles based on the NPPs.

The *Health Complaints Act 1995 (Tas)* also led to the establishment of a *Charter of Health Rights* which applies to a wide range of health service providers. The Charter sets out a range of rights for consumers and also provides that health service providers have the right to discuss the healthcare of a consumer with other providers if it is in the best interest of the consumer. There is an implication in the Charter that no patient consent is required for such discussions to take place, which arguably puts the Tasmanian regime at odds with NPP10 which implies that consent (or implied consent) is necessary.

Managed by the Tasmanian Ombudsman: <http://www.ombudsman.tas.gov.au/>



ACT

The *Health Records (Privacy and Access) Act 1997 (ACT)* removes health records in the ACT from the jurisdiction of the Office of the [Federal] Privacy Commissioner. The ACT Act establishes:

- 14 privacy principles that have been modified to suit the requirements of health records

Managed by the Office of the Privacy Commissioner (Australian):

http://www.privacy.gov.au/privacy_rights/laws/index.html#8

Northern Territory

The *Information Act 2002 (NT)* establishes:

- 10 Information Privacy Principles, based on the NPPs.

The Territory Health Service also published the *Information Privacy Code of Conduct* which establishes:

- 11 principles that are based on the IPPs in the Privacy Act.

Note that the Code removes the right of access by patients to healthcare records and treatment information.

Managed by the Office of the Information Commissioner: <http://www.privacy.nt.gov.au/>

A special note of caution regarding the Collection Principle (NPP 1)

Certain aspects of data collection may not be obvious and need to be understood. Privacy legislation generally does not give direction about the manner in which personal information is collected. No matter how personal information comes to be held by an organisation, privacy legislation may apply. So it is important that Divisions think beyond the confines of traditional overt collection of patient information and that they ensure that no matter how personal information is gathered, that proper privacy safeguards are in place.

Some of the less obvious ways in which personal information including health information may be collected include:

- creation of fresh evaluative information about individuals by their carers;
- sharing of health care and treatment information amongst carers;
- acquisition of information when one healthcare organisation merges with another;
- compilation of event logs relating to people accessing healthcare information; for instance, address details of people who has requested information about certain medical conditions;
- compilation of event logs relating to people accessing health related goods and services; for instance, the buying habits of people purchasing health food online could constitute sensitive health information; and
- call centre logs and temporary files can inadvertently include identifiable information pertaining to health conditions; great care must be taken to store or dispose of these securely.

Collection of Information for Business or Management Purposes

The Privacy Act 1988 (Commonwealth) and other legislation anticipates numerous scenarios 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. In general, re-use of personal information used for such purposes must remain consistent with the primary purpose of collection (for example, it was originally collected as part of a medical treatment) or secondary purposes that are reasonably related to the primary purpose. However, when personal information is also sensitive information, such as healthcare information, there is much less room for interpreting reuse beyond the primary purpose. Furthermore, there are higher expectations regarding the capture of the individual's consent when it comes to healthcare information.

Critically, the use any health information must be consistent with the individual's reasonable expectations as to how the organisation would use or disclose the information.

Divisions should err on the side of caution. Every reasonable effort should be made to inform all people who use a Division's services and provide personal information as to why it is being collected and how it is to be



used. When identifiable health information is collected by a Division indirectly, through a third party health organisation, the Division should consider alerting individuals concerned of the fact that their details are now being held.

De-identified Data

In general, privacy legislation only applies to data about individuals who can be readily identified, so using *de-identified* data where possible removes much of the regulatory burden associated with privacy.

However, it is important to ensure that the process of de-identification cannot be reasonably reversed. Permanently removing names and personal identifiers from health records is a necessary step in de-identification but may not be sufficient. There are numerous statistical and data matching techniques available that can help to re-identify persons associated with health information. When the “cell size” (number of people in the sample) is small, then re-identification may be possible based on fine grained characteristics, such as birth date, race, or specific medical conditions.

Divisions must take care not to accidentally disclose information about those agencies that provide information to them that could either disclose personal information about an individual or adversely affect the organisation providing them with information. For example, a GP with a significant case load of complex care high risk patients with diabetes could be identified having poor outcomes for people with diabetes. The Division therefore must ensure that GP identity is de-identified and the information is appropriately contextualised and explained when publicly releasing any materials.

Commercial in Confidence

It is also important for Divisions to understand that general practitioners, as business people, can sometimes have a commercial interest in the data their practices may hold. So in addition to the obligations imposed by privacy legislation, Divisions should heed these commercial interests and seek wherever possible the permission of the practice before re-using any of their data.

Research

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

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 (i.e. electronic or paper) must be stored safely and securely in line with NPP 4. A Division must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

Divisions may have to take specific advice from security experts as to what measures are reasonable and sensible in each context. The customary way to assess security measures is through a threat and risk assessment in line with such standards as AS 4360 Risk Management.



Part 2 – Case Studies

To assist Divisions in the practical application of the Privacy Legislation and associated principles three case studies are provided. When considering the case studies, Divisions should reflect upon how they would deal with similar situations and how their current policies would deal with the identified issues.

Case Study 1

A Division had a temporary administrative assistant to help it get National Performance Indicator (NPI) data collected and checked before it goes to the Department of Health and Ageing. The assistant remarks to another Divisional staff person that the HBA1C data from a particular sole practice has a very high number with levels over 7 and the Doctor concerned can't be doing a good job. They then discuss this observation socially with friends, one of whom writes for the local newspaper and publishes a story about the poor practice.

In this situation, there is a risk of a breach of the sole practitioner's privacy with potential disruptive consequences for all concerned. This situation highlights the need to ensure that new employees (whether temporary or not) are fully aware and comply with the requirements of the Privacy Act. The particular incident indicated a need to review the Division's induction processes and possibly its recruitment practices. It is the responsibility of the CEO to protect the privacy rights of their Division's members, their member's patients and their staff, to ensure that they do not make, even well intentioned errors, that could cause members or patient distress or result in complaints under the law.

Case Study 2

A Division's IT support officer agrees to help a practice analyse their chronic diseases data and extracts several hundred patient records out of the practice management system for analysis off site, copying the data to his notebook computer. The next day the support officer's car is stolen, together with his notebook computer.

In this situation, there is an uncontrolled risk of a severe privacy breach occurring. In situations such as this, third parties from Divisions or anywhere else should be given access to practice internal information only when a demonstrable need-to-know basis exists and after a non-disclosure agreement (if applicable) has been signed and authorised. Patient information must not be distributed to third parties without advance authorisation by the patient.

Third party information entrusted to the Division should be protected as if it were the practice's own information. When being used (and stored) in the office, laptop computers should be secured e.g. with locking cables, placed in lockable cabinets or secured via other locking systems.

Portable computers should not be left unattended and on flights, portable computers should be taken as hand luggage if possible. They should not be stored in a car. There should be a set of Division guidelines to clarify staff access to member's medical records. The guidelines should clarify who can access what information. All staff should be made aware of the guidelines.

Case Study 3

The Division is undertaking a study to look at health among people from Culturally and Linguistically Diverse Backgrounds (CALD). It has identified a range of GPs within the area that have a high proportion of patients from CALD backgrounds. The Division asks the GPs who are interested in the study to attend a meeting to be briefed on the purpose of study, how data is to be collected, analysed, reported and disposed of.

At this meeting, the GPs are asked to identify which language patients would most likely speak so that information packs and consent forms can be produced in the relevant languages. The GPs were also provided with a telephone number for a telephone interpreter service to ensure that the patients are provided information in a form that they can understand.



The doctors also raise the issue that many of their patients have come to Australia as refugees, often having experienced ethnic cleansing campaigns in their countries of origin. Given this experience, it is decided that the collection of potential identifiable CALD information would be significantly de-identified so as a cultural group could not be identified. In doing this, the Division is able to work with GPs to ensure that both the patients and GPs understand what information is being collected, how it is to be used and to respect the privacy and dignity of patients.



Part 3 - Privacy Checklist

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

| Task | Yes | No | Comment |
|---|-----|----|---------|
| Are you familiar with the 10 National Privacy Principles? (See Appendix 1) | | | |
| Have you made all staff within the Division aware of the Privacy Act and the 10 National Privacy Principles? If not, how do you intend to raise awareness? | | | |
| Have you formulated (or adopted) and promulgated a Privacy Policy? | | | |
| Has the Division's Board signed off on their privacy obligations and responsibilities? | | | |
| Does the Division have a designated Privacy Officer? | | | |
| Have you trained your staff in relation to the Division's privacy policy and associated procedures? | | | |
| Are you aware of the definition of 'sensitive information' and the special obligations that go with it? | | | |
| Does the Division have a sound (preferably documented) understanding of any and all cases of collection of sensitive information (i.e. identifiable health information)? | | | |
| Does the Division exchange personal information with external organisations or groups? If yes, is the Division aware of its responsibilities when doing so? | | | |
| Have you conducted a privacy audit of your Division's practices and procedures in relation to the handling of personal information? | | | |
| Have you conducted a recent security review of your Division's information management systems? | | | |
| Does the Division have procedures for alerting individuals when personal information about them is collected by the Division, and obtaining their consent where applicable? | | | |
| Is there a protocol for making people who provide personal information to the Division aware of their rights under the Privacy Act? | | | |
| Does the Division have procedures for handling requests to access and amend personal information? | | | |
| Does the Division have procedures 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? | | | |

(Adapted from; *Privacy Resource Handbook For all Medical Practitioners in the Private Sector* 1st Edition, 2002, published by RACGP)



References

Free copies of the Privacy Act and the National Privacy Principles, together with implementation guides, handbooks and templates can be found from many online resources, as follows:

1. Australian Capital Territory: Office of the Privacy Commissioner (Australian)
Accessed 28/03/2008. Available at: http://www.privacy.gov.au/privacy_rights/laws/index.html#8
2. General Practice Computing Group (GPCG) privacy resources. Accessed 28/03/2008.
Available at:
http://www.gpcg.org.au/index.php?option=com_content&task=category§ionid=4&id=19&Itemid=107
3. New South Wales Office of the NSW Privacy Commissioner.
Accessed 28/03/2008. Available at:
http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_index
4. Northern Territory: Office of the Information Commissioner
Accessed 28/03/2008. Available at: <http://www.privacy.nt.gov.au/>
5. Privacy Commissioner: Accessed 28/03/2008.
Available at: <http://www.privacy.gov.au>
6. Privacy Commissioner: List of State and Territory Laws compiled by the Privacy Commissioner;
Accessed 28/03/2008. Available at: http://www.privacy.gov.au/privacy_rights/laws/index.html - 1
7. Privacy Commissioner Health Issues and Fact Sheets compiled by the Privacy Commissioner;
Accessed 28/03/2008. Available at: <http://www.privacy.gov.au/health/index.html>
8. Queensland: Department of Justice and Attorney-General Accessed 28/03/2008.
Available at <http://www.privacy.qld.gov.au/>
9. South Australia: Privacy Committee. Accessed 28/03/2008.
Available at: <http://www.archives.sa.gov.au/privacy/committee.html>
10. Tasmania: Ombudsman. Accessed 28/03/2008.
Available at <http://www.ombudsman.tas.gov.au/>
11. Royal Australian College of General Practitioners (RACGP) privacy resources.
Accessed 28/03/2008. Available at: <http://www.racgp.org.au/privacy>
12. The Royal Australian College of General Practitioners and Committee of Presidents of Medical Colleges with the support of the General Practice Computing Group:

The Handbook for the Management of Health Information in Private Medical Practice,
1st Edition (2001), published by:

The Royal Australian College of General Practitioners
College House
1 Palmerston Crescent
SOUTH MELBOURNE VIC 3205
Accessed 28/03/2008.

Available at:

<http://www.racgp.org.au/Content/NavigationMenu/PracticeSupport/Privacy/Handbookforthemangementofhealthinformationinprivatepractice/20021014privacy.pdf>



Victoria: Office of the Victorian Privacy Commissioner. Accessed 28/03/2008.
Available at: <http://www.privacy.vic.gov.au/dir100/priweb.nsf>

13. Western Australia: Office of the Information Commissioner. Accessed on 28/03/2008.
Available at <http://www.foi.wa.gov.au/>

Disclaimer

The information contained in the “Privacy guidelines for reuse of information” tool is provided as a guide only and is not intended to be a substitute for independent professional advice. References to websites are provided for the user's convenience only and do not constitute Endorsement of material at those sites, or any associated organisation, product or service. The Commonwealth Department of Health and Ageing does not warrant or represent that the information contained in the “Privacy guidelines for reuse of information” toolkit is accurate, current or complete. Users should exercise their own independent skill or judgement or seek professional advice before relying on it. The Commonwealth Department of Health and Ageing does not accept any legal liability or responsibility for any injury, loss or damage incurred by the use of, or reliance on, or interpretation of, the information contained in the “Privacy guidelines for reuse of information” tool.



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



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;
 - (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 aim.

END of DOCUMENT