Privacy Policy

Policy version: 1.0

Acceptance Certificate:

Name	Title:	Signature:	Date:
Cameron Cox	Chief Executive Officer	Cameron Cox.	19/08/2015

Document Reviewers:

Cameron Cox	Chief Executive Officer	Signature: Cameron Cox.	Date: 19/08/2015
SWOP Committee		Signature: N/A	Date:
Indraveer Chatterjee	Principal Solicitor, HALC	Signature: 	Date: 23/07/2015

Table of Contents

1. Background

The confidentiality of our service users has been an underpinning philosophy and foundation of SWOP's work since its inception. SWOP supports the spirit of intent and complies with and where possible strives to exceed the requirements of the Privacy Act 1988 (Commonwealth).

2. Policy Statement

This policy applies to the whole of SWOP, the Board, staff, volunteers and contracted service partners.

SWOP's Privacy Policy outlines what happens to personal information collected by SWOP, how it is used and how a service user can find out what information SWOP holds about them. It also explains how a service user can have that information changed or altered if it is incorrect or out of date.

3. Applicable Legislation

3.1. Privacy Amendment (Enhancing Privacy Protection) Act 2012

The Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Privacy Amendment Act) introduced many significant changes to the Privacy Act. Both the Act and the Privacy Regulation 2013, made under the Privacy Act, commenced on 12 March 2014.

The *Privacy Amendment Act* includes a set of new, harmonised, privacy principles that will regulate the handling of personal information by both Australian government agencies and businesses. These new principles are called the Australian Privacy Principles (APPs). They will replace the existing National Privacy Principles (NPPs) that currently apply to businesses (including NGO's).

Under the changes, there are 13 new APPs. A number of the APPs are significantly different from the existing principles, including APP 7 on the use and disclosure of personal information for direct marketing, and APP 8 on cross-border disclosure of personal information.

The Act regulates how organisations such as SWOP should collect, keep, use and disclose personal information. SWOP complies with and, wherever possible, strives to exceed the requirements of the Act. SWOP complies with all of the APPs.

The APPs are in addition to existing legislation and guidelines which affect parts of the private sector.

The thirteen Australian Privacy Principles allow for individuals to exercise rights and choices about how their personal and health information is handled in the private health sector. The Act also gives people these rights over personal information held by other private sector organisations.

In addition, the National Health and Medical Research Council (NHMRC) has issued guidelines (s.95 and s.95A), approved by the Privacy Commissioner. These guidelines balance the protection of an individual's

health information with the need for ethically approved research using individuals' health data without consent.

Service users have the right to request access to their personal information and for it to be changed or altered if incorrect or out of date. Under special circumstances outlined in AAP 12, SWOP may refuse to allow a service user to see information held about them, but is required under the Act to explain why. The Act provides that a service user may make a complaint to SWOP or the Privacy Commissioner if they think their information is not used or held appropriately and in accordance with the Act.

3.2. Privacy Act 1988 (Cth)

The Privacy Act 1988 (Cth) (the "Act") sets out a service user's rights and SWOP's responsibility relating to any personal information held about them. The Act provides service users with the right to know what information is held about them, how SWOP will use that information and under what circumstances their personal information may be divulged to others.

3.3. Further Information on Federal Privacy Laws

The Office of the Australian Information Commissioner's web-site contains detailed information on privacy obligations.

3.4. New South Wales Privacy Laws

The Privacy and Personal Information Protection Act 1998 (PPIP Act) deals with how all New South Wales public sector agencies manage personal information. It also sets out the role of the NSW Information and Privacy Commission.

While the PPIP Act applies primarily to the New South Wales public sector, when private sector organisations contract with NSW government agencies to provide services to them, the terms of the contract will sometimes require the organisation to follow the Information Protection Principles (IPPs) in how it delivers those services.

The *Health Records and Information Privacy Act 2002* (HRIP Act) governs the handling of health information in the public sector, and it also regulates the handling of health information in the private sector in New South Wales.

The 15 health privacy principles (HPPs) are the key to the *Health Records and Information Privacy Act* (HRIP Act). They are legal obligations describing what organisations (NSW public and private sector) must do when they collect, hold, use and disclose health information. These roughly parallel the Federal principles.

For more information on the HRIP Act, see Appendix B.

Other relevant New South Wales laws include, but are not limited to:

- State Records Act 1998
- Public Health Act (NSW) 2010

4. Definitions

4.1. Personal Information

Personal information includes such things as a person's full name, date of birth, gender, address and other contact details. The Act recognises that information of a more sensitive nature may be collected by organisations such as SWOP in order to provide service users with, or refer them to particular services.

4.2. Sensitive Information

Sensitive information is a subset of personal information. It means information or opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, gender identification, criminal record or health information about an individual.

Appendix A provides a short summary that sets out clearly expressed policies on the way SWOP manages personal information. It must be made available to anyone who asks for it.

4.3. Enforcement related activity

Enforcement related activity means:

- the prevention, detection, investigation, prosecution or punishment of:
    - (i) criminal offences; or
    - (ii) breaches of a law imposing a penalty or sanction; or
- the conduct of surveillance activities, intelligence gathering activities or monitoring activities; or
- the conduct of protective or custodial activities; or
- the enforcement of laws relating to the confiscation of the proceeds of crime; or
- the protection of the public revenue; or
- the prevention, detection, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations; or
- the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders.

4.4. Permitted health situations

Under section 16B of the Privacy Amendment Act, a **permitted health situation** may provide an exemption to the requirements of AAP6 in relation to the health information of an individual.

4.4.1 Collection

A ***permitted health situation*** exists in relation to collection of the information is necessary to provide a

health service to the individual, and the collection is either required or authorised by or under an Australian law (other than this Act); or the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind SWOP.

A ***permitted health situation*** may also exist in relation to the collection of health information about an individual if the collection is necessary for research relevant to public health or safety; the compilation or analysis of statistics relevant to public health or public safety; or the management, funding or monitoring of SWOP as a health service.

However, the collection of personal information in these research-related circumstances is permitted only if the purposes above **cannot** be served by the collection of information about the individual that is de-identified information and it is impracticable for SWOP to obtain the individual's consent to the collection and;

- the collection is required by or under an Australian law (other than this Act); or
- the information is collected in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind SWOP; or
- the information is collected in accordance with guidelines approved under section 95A of the Privacy Act for these purposes.

4.4.2 Use or disclosure – research etc.

A ***permitted health situation*** may exist in relation to the use or disclosure by an organisation of health information about an individual if:

- the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety; and
- it is impracticable for the organisation to obtain the individual's consent to the use or disclosure; and
- the use or disclosure is conducted in accordance with guidelines approved under section 95A of the Privacy Act for the purposes of this paragraph; and
- in the case of disclosure—the organisation reasonably believes that the recipient of the information will not disclose the information, or personal information derived from that information.

4.4.3 Disclosure – responsible person for an individual

A ***permitted health situation*** may exist in relation to the disclosure by SWOP of health information about an individual if

- the organisation provides a health service to the individual; and
- the recipient of the information is a responsible person for the individual; and

- the individual
    - is physically or legally incapable of giving consent to the disclosure; or
    - physically cannot communicate consent to the disclosure; and
- another individual (the carer) providing the health service for SWOP is satisfied that either
    - the disclosure is necessary to provide appropriate care or treatment of the individual; or
    - the disclosure is made for compassionate reasons; and
- the disclosure cannot be contrary to any wish:
    - expressed by the individual before the individual became unable to give or communicate consent; and
    - of which the SWOP carer is aware, or of which the SWOP carer could reasonably be expected to be aware; and
- is limited to the extent reasonable and necessary to provide appropriate care or treatment of the individual; or
- the disclosure is made for compassionate reasons.

5. Summary of the Thirteen Australian Privacy Principles and their Application at SWOP*

APP 1 — Open and transparent management of personal information

Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.

- SWOP has a clearly expressed and up to date privacy policy (this document) that includes reasonable steps to ensure that the organisation complies with the APPs.
- This policy is available free of charge via SWOP's website. SWOP must take such steps as are reasonable to provide this policy in an alternate form when requested.

APP 2 — Anonymity and pseudonymity

Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.

- If it is lawful and practicable to do so, give people the option of interacting with SWOP anonymously or by using a pseudonym.

APP 3 — Collection of solicited personal information

Outlines when an APP entity can collect personal information that is solicited. It applies higher standards

to the collection of 'sensitive' information.

- Only collect personal information that is necessary or directly related to SWOP's functions or activities.
- Get consent to collect sensitive information unless specified exemptions apply.
- Use fair and lawful ways to collect personal information.
- Always collect personal information directly from an individual unless the person consents to collection of information from a third party or it is unreasonable or impracticable to do so.

APP 4 — Dealing with unsolicited personal information

Outlines how APP entities must deal with unsolicited personal information.

- The employee's manager will establish if the unsolicited information could have been collected under APP 3 above.
- The manager will destroy or de-identify the information if it could not have been collected under APP 3.

APP 5 — Notification of the collection of personal information

Outlines when and in what circumstances an APP entity that collects personal information must notify an individual of certain matters.

- At the time personal information is collected or as soon as practicable afterwards, SWOP will take reasonable steps to make an individual aware of:
    - who SWOP is and how to contact us;
    - the purpose(s) of the collection;
    - any collections from third parties;
    - consequences (if any) to the individual of non-collection;
    - SWOP's complaint handling process;
    - any potential overseas disclosure

APP 6 — Use or disclosure of personal information

Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.

- SWOP will only use or disclose personal information for a purpose other than the primary purpose for which it was collected if:
    - the other purpose of collection is directly related to the stated purpose; and
    - the service user would reasonably expect SWOP to use or disclose information for the related purpose; or
    - the service user gave permission for its use or disclosure.

- SWOP will only use or disclose information for a secondary purpose without a service user's consent, when:
    - SWOP reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
    - SWOP is required or authorised to do so by law or court/tribunal order;
    - SWOP reasonably believes that the use or disclosure of the information is reasonably necessary for enforcement related activities conducted by or on behalf of an enforcement body ;
    - SWOP has reason to suspect that unlawful activity, or misconduct of a serious nature relating to its functions or activities has been, is being or may be engaged in; and SWOP reasonably believes that the collection, use or disclosure is necessary in order for SWOP to take appropriate action in relation to the matter.
- Under limited exceptions, SWOP may permit the collection, use or disclosure of information for secondary purposes of:
    - locating a missing person;
    - establishing, exercising or defending a legal equitable claim;
    - confidential alternative dispute resolution.

APP 7 — Direct marketing

An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.

- SWOP prohibits the use or disclosure of personal information for direct marketing purposes, except where:
    - SWOP collected the information from the individual and the individual would reasonably expect SWOP to use or disclose the information for this purpose; and
    - The individual was given a simple means to request **not** to receive direct marketing communications from SWOP and the individual did not make such a request.
- This provision is subject to the operation of other direct marketing legislation, eg the Spam Act 2003.

APP 8 — Cross-border disclosure of personal information

Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.

- Under the legislation, SWOP may be held accountable for a breach of APPs by overseas recipients of personal information provided by SWOP. Therefore, SWOP exercises an

accountability approach for cross-border disclosures.

- SWOP will take reasonable steps to ensure overseas recipients do not breach APPs. **Any use or disclosure of personal information to an overseas entity must be approved in writing by the CEO.**

APP 9 — Adoption, use or disclosure of government related identifiers

Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.

- SWOP does not use identifiers or reference numbers assigned by other organisations or government departments or services (eg tax file number) unless required by Australian law or court order.

APP 10 — Quality of personal information

An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.

- Employees must take reasonable steps to ensure personal information collected, used or disclosed is:
    - Accurate
    - Up-to-date
    - Complete
- Employees should ensure that personal information that is used or disclosed is also relevant for the purpose of the use or disclosure.

APP 11 — Security of personal information

An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

- SWOP employees must take reasonable steps to protect the personal information held from misuse, interference and loss and from unauthorised access, modification or disclosure. This may include secure or locked storage, password protected systems or other means.
- If the personal information is no longer needed for any purpose for which SWOP may use or disclose it, the manager must take reasonable steps to destroy or permanently de-identify the personal information.

APP 12 — Access to personal information

Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific

exception applies.

- If an individual asks, SWOP will take reasonable steps to let them know, generally, what sort of personal information is held, the purposes for which it is held and how it is collected, used and disclosed.
- If an individual asks, SWOP will give access to the personal information held about them unless particular circumstances apply that allow limits to the extent of this access - these include:
    - the belief that giving access would pose a serious threat to the life, health or safety of any individual, or to public health and safety; or
    - the belief that giving access would have an unreasonable impact on the privacy of other individuals; or
    - the request is frivolous or vexatious;
    - the information relates to existing or anticipated legal proceedings between SWOP and the requester and would not be accessible via the processes of discovery in the proceedings; or
    - giving access would reveal the intentions of SWOP in relation to negotiations with the individual in such a way as to prejudice the negotiations; or
    - giving access would be unlawful; or
    - denying access is required or authorised under Australian law or via a court order; or
    - SWOP has reason to believe that unlawful activity or misconduct of a serious nature that relates to SWOP's functions or activities has been or is being engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
    - giving access would likely prejudice one or more enforcement related activities conducted by or on belhalf of an enforcement body; or
    - giving access would reveal evaluative information generated within SWOP in connection with a commercially sensitive decision-making process.
- SWOP is required to respond to requests for access of personal information within a reasonable timeframe.
- Access should be provided in the requested manner (where reasonable and practicable).
- Any charges for access to personal information must not be excessive, and must not apply to the making of the request.
- SWOP must give written reasons for :
    - the refusal to grant access (unless it would be unreasonable to do so); or

- the refusal to grant access in the manner requested;

as well as written information on how to make a complaint regarding the refusal.

APP 13 — Correction of personal information

Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

- SWOP must take 'reasonable steps' to correct personal information to ensure that it is accurate, up-to-date, complete, relevant and not misleading, if either:
  - SWOP is satisfied the information needs to be corrected; or
  - the individual requests correction.
- When refusing a request to correct the individual's information, SWOP must provide a written statement within a reasonable period setting out the reasons for refusal (unless it would be unreasonable to do so) and how to make a complaint regarding the refusal to correct the information.

This is a summary only and NOT a full statement of obligations. These are set out in the APPs themselves. The complete text of the Australian Privacy Principles may be found in OIPC Privacy fact sheet 17: Australian Privacy Principles.

6. Miscellaneous

Any questions relating to this policy should be addressed to your manager

7. Review of this Policy & Procedure

This policy will be reviewed at least once every four years.

8. Related Documents

- SWOP Change of Address Form
- SWOP Personal Information Inquiry Form

9. Policy History

Date	Reason for Change	Change Description	Author	Issue No:
	Creation		Michelle Wood	0.1
14/05/15	Approved	Approved by SWOP Governance Committee, subject to sign off by lawyer	Kylie Tattersall / SWOP Governance Committee	1.0
19/08/15	Edited	Integration of edits advised by lawyer (pre-approved by Committee)	Michelle Wood	0.2

APPENDIX A: FAQ SHEET FOR SERVICE USERS

SWOP MANAGEMENT OF PERSONAL INFORMATION

Openness

SWOP's Privacy Policy and this FAQ Sheet are publicly available through SWOP's website. Copies of this FAQ may also be obtained through the contact details provided at the end of this document.

On request by an individual, SWOP will take reasonable steps to let that individual know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.

Notification and Collection

When collecting personal information, SWOP will take reasonable steps to make an individual aware of:

- What SWOP is and how to contact us; and
- How to gain access to the information; and
- Why the information is collected; and
- To whom (if anyone) SWOP may disclose the information; and
- Any law that requires the information to be collected; and
- the consequences (if any) to the individual if all or part of the information is not provided; and
- SWOP's complaint handling process;
- any potential overseas disclosure.

SWOP uses fair and lawful ways to collect personal information and only collects personal information that is necessary for our functions or activities. We collect personal information directly from the individual whenever it is reasonable and practicable to do so.

If SWOP collects personal information about an individual from someone else, we will take reasonable steps to ensure that the individual is made aware of the matters listed below, except to the extent that making the individual aware of the matters would pose a serious threat to the life, health or safety of any individual or to public health and safety.

SWOP always gets consent to collect sensitive information unless specified exemptions apply.

Use and Disclosure

Information about an individual will only be used or disclosed to others by SWOP in ways which meet that individual's expectations or are required by law.

SWOP will only use or disclose personal information for a purpose other than the primary purpose for which it was collected if:

- the other purpose of collection is directly related to the stated purpose; and
- the service user would reasonably expect SWOP to use or disclose information for the related

purpose; or

- the service user gave permission for its use or disclosure.

SWOP will only use or disclose personal information without the individual's consent, when:

- it is in the interest of an individual's health, life or safety;
- in the interest of public health or safety; or
- SWOP is required or authorised to do so by law.

SWOP may disclose health information about an individual to a person responsible for that individual such as a legally appointed guardian.

Under limited exceptions, SWOP may permit the collection, use or disclosure of information for secondary purposes of:

- locating a missing person;
- establishing, exercising or defending a legal equitable claim;
- confidential alternative dispute resolution.

SWOP prohibits the use or disclosure of your personal information for direct marketing purposes, except where you would reasonably expect SWOP to use or disclose the information for this purpose (e.g. service promotion); and you were given the option not to receive direct marketing communications from SWOP and you chose not to make such a request.

Data Quality

SWOP will take all reasonable steps to ensure that personal information collected, used or disclosed about a service user is as appropriate, accurate and current as possible.

Data Security

SWOP undertakes to ensure that all personal information is kept in a secure place or manner. We will take all reasonable steps to protect service user information from misuse, loss, unauthorised or unnecessary access, interference, alteration or disclosure. SWOP undertakes to destroy or de-identify personal information when it is no longer required for any purpose or by law.

Access and Correction

Access to an individual's information is limited to those SWOP personnel (staff or volunteers) who require the information for the effective provision of a service to that individual or those specifically authorised at the individual's request. SWOP personnel may not divulge any identifying information about a service user to others except where necessary to provide appropriate service to that individual.

SWOP will provide individuals with access to their personal information upon request. The individual may arrange an appointment to view their personal information or they may request a written copy. To obtain access to, or copies of, or to correct or up-date their personal information a service user will need to complete a 'Personal Information Inquiry' form. This form is available by written or telephone request or

from www.swop.org.au.

Under some circumstances, it may be inappropriate for SWOP to provide an individual access to their personal information (e.g. providing access would pose a serious threat to the life or health of any individual; or would have an unreasonable impact upon the privacy of other individuals). SWOP will provide reasons for any denial of access or a refusal to correct personal information.

On request, we will correct contact details, either over the phone, face-to-face or the individual may complete a 'Change of Address' form. This form is available by written or telephone request or from www.swop.org.au.

Complaints

SWOP has a complaints procedure for anyone who believes their information is not being handled properly or in accordance with this policy. A copy of SWOP's complaints procedure may also be obtained through the same contacts. A complaint may also be lodged with the Privacy Commissioner.

Identifiers

SWOP does not use identifiers or reference numbers assigned by other organisations or government departments or services (e.g. tax file number).

SWOP does not release its own membership or service user case file numbers to other organisations. Nor do we divulge any information that may in any way identify a particular individual to other organisations, or to SWOP staff or volunteers.

Anonymity

Wherever practicable and lawful, SWOP will provide a service user with the option of interacting with SWOP anonymously or through use of a psueudonym.

Transborder Data Flows

SWOP will only send service user information to a third party interstate or in a foreign country with that service user's prior consent or where required by law.

Sensitive Information

SWOP will not collect sensitive information about a service user without their consent unless, the collection is necessary to prevent or lessen a serious threat to health or life, or the collection is required by law.

SWOP in some instances may collect information without an individual's consent if the person concerned is physically or legally incapable of giving consent.

SWOP may also collect sensitive information without consent in accordance with rules established by competent health or medical bodies that deal with the obligations of professional confidentiality (e.g. service user case notes kept about counselling sessions with professionally recognised psychotherapists or session case notes kept by counsellors).

Contacts

For any questions about SWOP's Privacy Policy contact the Corporate Services Team Leader.

Copies of SWOP's Privacy Policy, Personal Information Inquiry forms or Change of Address forms may be down-loaded from our web-site http://www.swop.org.au or by telephoning the SWOP office.

APPENDIX B: FAQ ON HRIP ACT

Brief introduction to the HRIP Act

The *Health Records and Information Privacy Act 2002* (or HRIP Act) protects the privacy of health information in NSW.

The HRIP Act governs the handling of health information in both the public and private sectors in NSW. This includes hospitals whether public or private, doctors, and other health care organisations. It also includes other organisations that have any type of health information. This can be as varied as a university that undertakes research, or a gymnasium that records information about a person's health and injuries.

The HRIP Act contains 15 health privacy principles (HPPs) outlining how health information must be collected, stored, used and disclosed. The health privacy principles can be grouped into seven main headings - collection, storage, access & accuracy, use, disclosure, identifiers & anonymity, and transferrals & linkage. These are legal obligations that must be followed although the HRIP Act provides for a number of legal exemptions from these principles.

The HRIP Act also sets out how complaints regarding the handling of health information can be dealt with.

Definitions

What is health information?

'Health information' is a specific type of personal information. Health information includes personal information that is information or an opinion about the physical or mental health or a disability of an individual.

Health information *also* includes personal information that is information or an opinion about:

- a health service provided, or to be provided, to an individual
- an individual's express wishes about the future provision of health services to him or her
- other personal information collected in connection with the donation of human tissue
- genetic information that is or could be predictive of the health of an individual or their relatives or descendants.

If your organisation is a health service provider, 'health information' includes all of the above *plus* any other personal information collected to provide, or in providing a health service.

'Health information' is defined in section 6 of the HRIP Act.

What is a health service provider?

A "health service provider" means an organisation that provides a health service. According to the definitions outlined in the HRIP Act, a "health service" includes the following services, whether provided as public or private services:

(a) medical, hospital, nursing and midwifery services,

(b) dental services,

(c) mental health services,

(d) pharmaceutical services,

(e) ambulance services,

(f) community health services,

(g) health education services,

(h) welfare services necessary to implement any services referred to in paragraphs (a)-(g),

(i) services provided in connection with Aboriginal and Torres Strait Islander health practices and medical radiation practices,

(j) Chinese medicine, chiropractic, occupational therapy, optometry, osteopathy, physiotherapy, podiatry and psychology services,

(j1) optical dispensing, dietitian, massage therapy, naturopathy, acupuncture, speech therapy, audiology and audiometry services,

(k) services provided in other alternative health care fields in the course of providing health care,

(l) a service prescribed by the regulations as a health service for the purposes of this Act.

For more information see the definitions in Part 1 of the HRIP Act.

What is a private sector person or organisation?

The HRIP Act applies to both individual people and organisations in the private sector. The types of organisations covered are body corporates, partnerships, trusts and unincorporated associations.

Individuals and organisations that will be regulated by the HRIP Act are:

- health service providers of any size (for example, an individual GP, a partnership of physiotherapists or a large private hospital), and
- organisations that handle health information and have a turnover of more than $3 million per annum (for example, an insurance company).

Health privacy principles at a glance

The 15 health privacy principles (HPPs) are the key to the *Health Records and Information Privacy Act* (HRIP Act). They are legal obligations describing what organisations (NSW public and private sector) must do when they collect, hold, use and disclose health information.

Collection

1. Lawful – Only collect health information for a lawful purpose that is directly related to the agency or organisation's activities and necessary for that purpose.

2. Relevant – Ensure the health information is relevant, accurate, not excessive, up-to-date and that the collection does not unreasonably intrude into the personal affairs of a person.

3. Direct – Only collect health information directly from a person concerned, unless it is

unreasonable or impracticable to do so. See the handbook on Health Privacy for an explanation of "unreasonable" and "impracticable". *Visit http://www.ipc.nsw.gov.au for definitions*.

4. Open – Inform a person as to why you are collecting health information, what you will do with it, and who else may see it. Tell the person how they can view and correct their health information and any consequences that will occur if they decide not to provide their information to you.

If you collect health information about a person from a third party you must still take reasonable steps to notify the person that this has occurred.

Storage

5. Secure – Ensure the health information is stored securely, not kept any longer than necessary, and disposed of appropriately. Health information should be protected from unauthorised access, use or disclosure. (**Note**: private sector organisations should also refer to section 25 of the *HRIP Act* for further provisions relating to retention).

Access & Accuracy

6. Transparent – Explain to the person what health information is being stored, the reasons it is being used and any rights they have to access it.

7. Accessible – Allow a person to access their health information without unreasonable delay or expense. (Note: private sector organisations should also refer to sections 26-32 of the HRIP Act for further provisions relating to access).

8. Correct – Allow a person to update, correct or amend their personal information where necessary. (Note: private sector organisations should also refer to sections 33-37 of the HRIP Act for further provisions relating to amendment).

9. Accurate – Ensure that the health information is relevant and accurate before using it.

Use

10. Limited – Only use health information for the purpose for which it was collected or for a directly related purpose, which a person would expect. Otherwise, you would generally need their consent to use the health information for a secondary purpose.

Disclosure

11. Limited -

Only disclose health information for the purpose for which it was collected, or for a directly related purpose that a person would expect. Otherwise, you would generally need their consent. (Note: see HPP 10).

Identifiers & Anonymity

12. Not identified – Only identify people by using unique identifiers if it is reasonably necessary to carry out your functions efficiently.

13. Anonymous – Give the person the option of receiving services from you anonymously, where this is lawful and practicable.

Transferrals & Linkage

14. Controlled – Only transfer health information outside New South Wales in accordance with HPP 14.

15. Authorised – Only use health records linkage systems if the person has provided or expressed their consent.

For more information

Contact the Information and Privacy Commission:

Freecall: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Website: www.ipc.nsw.gov.au