handbook

Health Records and Information Privacy Act 2002 (NSW)

Handbook to health privacy

privacynsw

CONTENTS

PART 1: INTRODUCTION AND KEY CONCEPTS

PART 2: YOUR LEGAL OBLIGATIONS UNDER THE HRIP ACT - THE 15 HEALTH PRIVACY PRINCIPLES (HPPS)

Part 1: Introduction and Key Concepts

1.1 BACKGROUND

Who is this handbook for?

The *Health Records and Information Privacy Act 2002 (NSW)* (the HRIP Act) regulates the collection and handling of people's health information by New South Wales public and private sector organisations. It applies to organisations that are health service providers or that collect, hold or use health information. The HRIP Act is fully operational from 1 September 2004.

This handbook is for individuals and organisations covered by the HRIP Act. We have written it to help you understand and comply with your legal obligations under the HRIP Act. This handbook contains plain English explanations of the key terms, and provides practical examples of how the HRIP Act might apply in some common scenarios. References to relevant sections of the HRIP Act have been included so that you can read this handbook and the HRIP Act together.

We have addressed the reader directly using the word 'you', however sometimes 'the organisation' is the better term. Where you see:

a **flag symbol**, it means that the information is specific to organisations in the **public** sector

a **pointed finger symbol,** it means that the information is specific to organisations in the **private** sector.

At the time of writing this handbook, no case law exists on the HRIP Act. Accordingly the information contained in this handbook is Privacy NSW's interpretation of the HRIP Act only.

The information is advisory, not legally binding, and should not be used as a substitute for legal advice.

The HRIP Act at a glance

The HRIP Act protects the privacy of people's health information. It does this by requiring those who handle health information to comply with **15 Health Privacy Principles (HPPs).** The 15 HPPs are the key to the HRIP Act. They are legal obligations describing what you must do when you collect, store, use or disclose health information. Privacy NSW recommends that you familiarise yourself with the 15 HPPs. The 15 HPPs are contained in Schedule 1, which is located at the end of the HRIP Act.

If you are based in the private sector, you will also need to know about the special private sector provisions in Part 4 of the HRIP Act. These provisions are in addition to, and expand upon, the 15 HPPs.

A summary of the 15 HPPs is set out on the following page. You will find a more detailed discussion of your obligations under the 15 HPPs, and the special private sector provisions, set out in **Part 2** of this handbook.

The Health Privacy Principles (HPPs) - Summary for organisations

Collection

1. **Lawful –** only collect health information for a lawful purpose. Only collect health information if it is directly related to the organisation's activities and necessary for that purpose.
2. **Relevant –** ensure that the health information is relevant, not excessive, accurate and up to date. Ensure that the collection does not unreasonably intrude into the personal affairs of the individual.
3. **Direct –** only collect health information directly from the person concerned, unless it is unreasonable or impracticable to do so. See the Handbook to Health Privacy for an explanation of "unreasonable" and "impracticable".
4. **Open –** inform the person as to why you are collecting health information about them, what you will do with the health information, and who else might see it. Tell the person how they can see and correct their health information, and any consequences, if they decide not to provide their information to you.
   If you collect health information about a person from someone else, you must still take reasonable steps to ensure that the person has been notified as described above.

Storage

5. **Secure –** ensure that health information is stored securely, not kept any longer than necessary, and disposed of appropriately. 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 instructions).

Access & Accuracy

6. **Transparent –** explain to the person what health information about them is being stored, why it is being used and any rights they have to access it.
7. **Accessible –** allow people 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 instructions).
8. **Correct –** allow people to update, correct or amend their health information where necessary (Note: private sector organisations should also refer to sections 33-37 of the HRIP Act for further instructions).
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 a directly related purpose that the person would expect. Otherwise, you generally need their consent.

Disclosure

11. **Limited -** only disclose health information for the purpose for which it was collected, or a directly related purpose that the person would expect. Otherwise, you generally need their consent.

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 people 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 –** people must expressly consent to participate in any system that links health records across more than one organisation. Only include health information about them, or disclose their identifier for the purpose of the health records linkage system, if they have expressly consented to this.

Why a separate law to protect health information?

Health information is a highly sensitive type of personal information. Health records often reveal more intimate, private and comprehensive details about a person than can be found in any other records maintained about them.

Given the personal and sensitive nature of health information, people are keen to see that the privacy of their health information is protected. They need to be satisfied whenever they use a health service or provide their health information to any other organisation, that the information will remain confidential. Without such confidence, people may not seek the health care they need. Alternatively, they may provide inaccurate and incomplete information.

In light of this, the NSW government developed the HRIP Act to provide specific and precise statutory protection for people's health information. The HRIP Act applies to both the public and private sector, insuring a consistent approach to the management of health information throughout NSW.

1.2 COVERAGE OF THE HRIP ACT

What information does the HRIP Act protect?

The HRIP Act protects the privacy of people's health information.

Health information:

See sections 5 and 6 of the *Health Records and Information Privacy Act 2002 (NSW)*

☐ ***Identifies a person***

Health information is a particular type of personal information[1]. Personal information is information that identifies a person. The person does not have to be clearly identified in the information. It is sufficient that their identity can be reasonably ascertained from the information.

Example:

In a small town, a medical report containing a person's date of birth, sex, and medical condition could conceivably lead to identification of the person. In this context, the information would be personal information.

If a person's identity cannot reasonably be ascertained from the information, then it is not personal information and is not covered by the HRIP Act.

Example:

Statistical data sets and other aggregated information that does not have the potential to identify a person, is not personal information and is not covered by the HRIP Act.

☐ ***Relates to a person's health or their health services***

Health information is personal information or an opinion about:

- a person's physical or mental health or disability, or
- a person's express wishes about the future provision of health services for themselves, or
- a health service provided, or to be provided to a person

It includes personal information, such as:

- genetic information about a person arising from a health service provided to them, that predicts or could predict the health of that person or of their siblings, relatives or descendants.

☐ ***Includes other personal information collected in providing a health service***

Health information also includes other personal information that is not of itself health-related, but which has been:

- collected to provide, or in providing, a health service[2], or
- collected in connection with a person's decision to donate body parts, organs or body substances.

Example:

- *name, address and contact details*
- *family details social circumstances*
- *employment details*
- *financial details*

Ordinarily this kind of information would not be health information because it is not, in of itself heath-related. However, if it has been collected in the course of providing a health service, or in connection with a person's donor decision, the information is classified as health information, and is protected by the HRIP Act.

Tip for Compliance:

If you or your organisation is a health service provider, this means that any information in identifiable form about a patient or a third party that you collect in the course of providing a health service will be classified as health information and will be protected by the HRIP Act.

Health information can be in any form:

- ☐ ***Paper, electronic, audio, visual etc***

The HRIP Act applies to all health information, regardless of the form it is in[3].
Paper, electronic, audio, visual and other types of health information are treated in exactly the same way under the HRIP Act.

- ☐ ***Does not need to be recorded in a material form***

Health information does not need to be recorded in a material form[4]. Unlike some laws (for example the *Freedom of Information Act 1989*) which relate only to documents, the coverage of the HRIP Act is much broader. There is also legal authority to suggest that coverage extends to information held in the mind of employees, when acquired in the course of their employment[5].

What about health information collected prior to the commencement of the HRIP Act?

See **section 19** of the *Health Records and Information Privacy Act 2002 (NSW)*

The HRIP Act is fully operational from 1 September 2004. The 15 HPPs generally apply to all health information, even if it was collected before 1 September 2004.

However some of the HPPs apply only to health information collected after 1 September 2004. These include HPP 1, HPP 2, HPP 3 and HPP 4 (on collection), and HPP 15 (on the linkage of health records). HPP 13 (on anonymity) applies only to transactions entered into after 1 September 2004.

HPP 7 (on access)[6] and HPP 8 (on amendment)[7] apply to all health information collected after 1 September 2004, and to certain health information[8] collected before 1 September 2004.

What information is not protected?

See section 5(3) of the *Health Records and Information Privacy Act 2002 (NSW)*

Health information about a person who has been dead for more than 30 years
The HRIP Act does not cover health information about a person who has been dead for more than 30 years[9].

Some employee-related health information
The HRIP Act does not cover some employee-related health information. The exact scope of this exemption differs depending on whether the organisation holding the health information is a public or private sector organisation (see below). However, as a matter of best practice and sensible risk management, Privacy NSW encourages organisations to handle all their employee-related health information in accordance with the HRIP Act.

☐ ***Public sector: 'information or an opinion about an individual's suitability for appointment or employment'***

In the public sector, the HRIP Act does not apply to 'information or an opinion about an individual's suitability for appointment or employment as a public sector official'.[10] This exemption is taken from the *Privacy and Personal Information Protection Act 1998.*

Example 1:

Question:
Bill undergoes a pre-employment medical check to assess his suitability for a public sector job in which he would be required to operate heavy machinery. Are the results of the pre-employment medical check protected by the HRIP Act?

Answer:
No. The results are not protected by the HRIP Act because the HRIP Act does not cover 'information or an opinion about an individual's suitability for appointment or employment as a public sector official'.

Example 2:

Question:
Bill then applies for a clerical job in the public sector. All candidates are required to undergo a pre-employment medical check. Are the results protected by the HRIP Act?

Answer:
Unlike the first example, where Bill's health was potentially relevant to his ability to do the job (eg. a person's epilepsy may render them unsuitable to operate heavy machinery), here the relevance of Bill's health to his suitability for the job is less clear. It is likely that the results would be protected by the HRIP Act because they do not constitute 'information or an opinion about an individual's suitability for appointment or employment as a public sector official'. It is also arguable that requiring Bill to do a pre-employment medical check for a clerical role is an unnecessary and excessive collection of health information potentially in breach of HPPs 1 and 2.

☐ ***Private sector: 'information about an individual that forms part of an employee record'***

In the private sector, the HRIP Act does not apply to 'information about an individual that forms part of an employee record'.[11]

This exemption is taken from the Federal *Privacy Act 1988*. It means that the HRIP Act does not protect health information held by a private sector employer about its current and former employees, where that information is held in employee records. However the HRIP Act does protect health information about applicants for private sector employment who have not entered into an employment relationship with the private sector organisation.

Example:

Question:
Bill undergoes a pre-employment medical check for a private sector job in which he would be required to operate heavy machinery. Are the results of the pre-employment medical check protected by the HRIP Act?

Answer:
The results are not protected by the HRIP Act, if Bill accepts the job and the information forms part of his employee record. However, if Bill is not offered the job or decides not to take up the position, the results of his pre-employment medical check are protected by the HRIP Act. This is because Bill is not an employee, and the exemption only applies to information that forms part of an employee record.

Certain other health information

The HRIP Act does not apply to certain other types of health information including:

- Health information that is generally available to the public, for example in a generally available publication, library, or the NSW State Archives.
- Health information that might be specially protected under other laws, such as a Protected Disclosure, information about a witness on a protected witness program, or information obtained during a special police operations.

For a complete list of exemptions to coverage, please refer to section 5(3)(a)-(o) of the HRIP Act.

What about de-identified information?

The HRIP Act applies to information that identifies a person, or from which a person's identity can reasonably be ascertained. Information that cannot be identified with any person raises far fewer privacy concerns and does not attract the protection of the HRIP Act. This means that you can generally use, or disclose de-identified information,[12] more freely and for a broader range of purposes.

Best Practice Tip:

Although de-identified information raises fewer privacy concerns, Privacy NSW recommends that you still notify people of potential uses of their de-identified data in the interests of transparency. For example, if you regularly provide de-identified health data to a university for research purposes then, you should make reference to this in your privacy policy, or notify the person at the time you collect their health information.

Who must comply with the HRIP Act?

You must comply with the HRIP Act if:

- you are a health service provider or
- you collect, hold or use health information

The HRIP Act applies to both the NSW public and private sector.

NSW organisations (includes individuals)

See **section 4** of the *Health Records and Information Privacy Act 2002 (NSW)*

The HRIP Act applies to organisations that are health service providers or that collect, hold or use health information. An 'organisation' is defined as a public sector agency or a private sector person. This means that individuals (such as GPs) are covered by the HRIP Act as private sector persons. It also means that the HRIP Act applies to both the NSW public and private sector.

☐ ***Public sector agency***

The term 'public sector agency'[13] includes most NSW State government departments and statutory authorities, and all local and county councils in NSW.

Tip for Compliance:

In the public health system, the public sector agency is the Area Health Service, not the hospital.

Example:

Question: Jane believes that a particular employee in a public sector agency breached her health privacy. Is this situation covered by the HRIP Act?

Answer: Yes. The HRIP Act applies to public sector agencies. This includes employees of public sector agencies. Employees must handle health information in accordance with the HRIP Act. The public sector agency is responsible for any privacy breaches committed by its employees.

☐ ***Private sector person***

The term 'private sector person'[14] is defined as a natural person (for example a GP, physiotherapist, optometrist), a body corporate (including state-owned corporations), a partnership, a trust or any unincorporated association or body.

Tip for Compliance:

Not-for-profit organisations and non-government organisations will often come within the definition of private sector person.

NSW organisations that are health service providers

The HRIP Act applies to all health service providers.

☐ ***What is a health service provider?***

See section 4 of the *Health Records and Information Privacy Act 2002 (NSW)*

Health service providers provide a health service. 'Health service' is defined in section 4 of the HRIP Act to mean any of the following services, whether provided as public or private services:

- medical, hospital, nursing, dental, mental health, pharmaceutical, ambulance, community health, health education services
- welfare services necessary to implement any of the above services
- services provided by podiatrists, chiropractors, osteopaths, optometrists, physiotherapists, psychologists and optical dispensers in the course of providing health care
- services provided by dieticians, masseurs, naturopaths, acupuncturists, occupational therapists, speech therapists, audiologists, audiometrists and radiographers in the course of providing health care
- services provided in other alternative health care fields in the course of providing health care

Other NSW organisations that collect, hold or use health information

The HRIP Act also applies to other organisations that collect, hold or use health information.

Tip for Compliance:

Even if your organisation is not a health service provider, chances are it will still collect, hold or use some health information. Most organisations handle health information in some capacity, usually about clients or employees. As a risk management tool, it may be useful to undertake an audit of your organisation's processes to identify how and where your organisation handles health information, and change processes where necessary.

☐ ***When does an organisation 'collect, hold or use' health information?***

An organisation 'collects' health information if it gathers, acquires or obtains it directly from the person to whom it relates or from another source. For more on collection, see **Part 2.1** of this handbook.

An organisation 'holds'[15] health information if the information is in the organisation's possession or control, or in the possession or control of a person employed, or engaged by, the organisation.

An organisation 'uses' health information when it communicates or handles it within the organisation. For more on use, see **Part 2.3** of this handbook.

Exemption for small business operators

Businesses with an annual turnover of $3 million or less are exempt from complying with the HRIP Act unless the business provides a health service, or is related to another business (for example it is a holding company or subsidiary) that has an annual turnover of more than $3 million[16]. The meaning of the words 'small business operator' in the HRIP Act is taken from section 6D of the *Privacy Act 1988* (Cth)

Example:

Question:
Is a chiropractor with an annual turnover of less than $3 million exempt from complying with the HRIP Act?

Answer:
No. A chiropractor is a health service provider. All health services providers are covered by the HRIP Act, regardless of their annual turnover.

Best Practice Tip:

Small business operators with an annual turnover of less than $3 million may still choose to opt in to the HRIP Act

How does the HRIP Act relate to existing laws, codes and guidelines?

Relationship with professional and ethical codes and standards

If you are already bound by existing professional and ethical codes of practice, you will continue to be bound by these. The HRIP Act is intended to support and operate alongside existing professional and ethical codes of practice.

Relationship with confidentiality

Health information has traditionally been protected by the doctrine of confidentiality. The obligation of confidentiality is owed to the person who provides the information. In some cases this will mean that the obligation is owed to the person to whom the information relates, however in other cases it will mean that the obligation is owed to another health practitioner or organisation.

Privacy continues to respect and support the principle of confidentiality. Privacy, however, approaches things a little differently. Privacy recognises that health practitioners today interact with a host of others, and that health information is handled by a broad spectrum of people including pharmacists, support staff, lawyers and employers. Not all of the people who handle health information are bound by a duty of confidentiality. Privacy legislation attempts to cover the wide range of ways that health information is handled. It does this by entitling the person, who is the subject of the health information, to have the greatest possible control over the flow of their own information. Privacy is an obligation to the subject of the information. The obligation exists regardless of who actually provided the information.

What if you have obligations under the Federal Privacy Act and the HRIP Act?

If you are from the private sector, you may have obligations under both the Federal *Privacy Act 1988* and the HRIP Act. If you have obligations under both Acts, then you should comply with both Acts concurrently. This will be possible in most cases. The underlying principles of the two pieces of legislation are the same, and the privacy protections are similar. However, the Australian Constitution says that where a law of the State is inconsistent with a law of the Commonwealth, the latter will prevail to the extent of the inconsistency.

What if you have obligations under the PPIP Act and the HRIP Act?

NSW public sector agencies will have obligations under both the *Privacy and Personal Information Protection Act 1998* (the PPIP Act) and the HRIP Act. The HRIP Act takes health information out of the PPIP Act and gives it specific protection. However, the PPIP Act will continue to apply to all other personal information that is not health information.

The HRIP Act and the PPIP Act are designed to stand side-by-side and complement each other. Public sector agencies should not have any difficulties complying with both Acts concurrently.

What if you are required by another law to collect, use, disclose or hold health information?

You may already have obligations to collect, use, disclose or hold health information under other laws. For example you might be required to:

- disclose health information to the Department of Community Services (DOCS) where a child or young person is at risk of harm under section 23 of the *Children and Young Persons (Care and Protection) Act 1998*
- disclose health information involving notifiable diseases pursuant to the *Public Health Act 1991*
- retain health information in accordance with the *State Records Act 1998*.

The HRIP Act does not override these other laws. You can continue to collect, use, disclose or hold health information as authorised, required, or permitted under any other State, Territory or Commonwealth laws[17].

1.3 OBTAINING A PERSON'S CONSENT TO HANDLE THEIR HEALTH INFORMATION

Consent is an important concept under the HRIP Act, and is a good guiding principle when you handle a person's health information.

Privacy NSW is of the view that wherever possible you should obtain the person's consent before collecting, using or disclosing their health information. Provided you have their valid consent, you have permission to use the information appropriately. Gaining consent is not only best practice in terms of privacy protection, but is also sensible risk management.

You should respect the person's right to determine how their health information is collected, used or disclosed, and provide them with the necessary information to enable them to exercise this right. Consent is only valid where it is fully informed, and where the person has the capacity to give it.

Elements of consent

This section explains the concept of consent as it relates to the handling of health information. It does not encompass consent to medical or dental treatment.

The term 'consent' is not defined in the HRIP Act. However it is Privacy NSW's view that for consent to be valid it must be voluntary, informed, specific, current, and given by a person who has the capacity to give it[18].

☐ ***Consent must be voluntary***

A person must be free to exercise genuine choice about whether to give or withhold consent. Consent must be given without coercion or threat. Sufficient time to must be allowed to understand the request and, if appropriate, take advice.

☐ ***Consent must be informed***

Generally, a person must have reasonable knowledge of all the relevant facts before they give or refuse consent. Providing incorrect or misleading information may mean that a person's consent is invalid.

Examples of relevant facts include:

- the purpose of collecting the health information
- who will have access to what parts of the health information
- what the recipient will use the health information for
- who the health information will be passed on to
- whether providing the health information is voluntary or required by law
- the consequences of giving or refusing consent

Tip for Compliance:

*You are required by **HPP 4** to notify the person of the above points when you collect health information about them anyway.*

☐ ***Consent must be specific***

Consent must be reasonably specific. Reliance on general, blanket or bundled consents can be problematic.

Tip for Compliance:

When drafting consent forms you should avoid 'bundled' consent. A consent form asking a person to tick one box to indicate their consent to multiple items (e.g. consent to treatment, consent to share their health information with relevant members of the treating team, and consent to use or disclose their details for fundraising purposes) is inappropriate. It is preferable that the consent form asks the person to tick separate boxes indicating their consent to each request.

☐ ***Consent must be current***

Consent has a 'use-by' date. Consent given in particular circumstances cannot be assumed to endure indefinitely with the passage of time and changes of circumstance. Good practice is to inform the person of a specified period for which the consent will be relied on in the absence of any material change of circumstances that the organisation knows or ought reasonably to know. Organisations should also make it clear that a person is entitled to change their mind and revoke consent later on.

Notifying a person is not the same as seeking their consent

Notifying a person of what you intend to do with their health information (for example by way of a standard brochure, form, or privacy policy) is not the same as seeking their consent to do those things.

HPP 4 requires you to notify a person of certain matters, including details of who you would normally provide their health information to. There is no doubt that if people are told who is likely to see their health information and what it will be used for, they are less likely to be surprised or angered when their health information is handled in that way. However, unless you actually give the person the choice of agreeing or disagreeing to what you propose, you are not seeking their consent.

Accordingly, fulfilling your notification obligations under HPP 4 is not the same as seeking a person's consent. Fulfilling your notification obligations under HPP 4 merely equips the person with the necessary knowledge to give or withhold informed consent. However, if you have notified the person that their information could be used or disclosed in a particular way, then there is a more persuasive argument that such a use or disclosure would be within the person's 'reasonable expectations'. This would put you in a better position to rely on the 'directly related secondary purpose within the reasonable expectations of the individual' exemption to use and disclosure in **HPPs 10(1)(b)** and **11(1)(b).** For more information, see **Part 2.3** of this handbook.

Is express or implied consent required?

Under the HRIP Act, consent may usually be either express or implied. It is generally preferable to seek express consent, although it will depend on the nature of the health information and the proposed conduct.

In two circumstances the HRIP Act specifically requires express consent from the person. These are:

- under HPP 4, where a person can expressly consent to waive their right to be notified when health information is collected about them, and
- under HPP 15, where a person's express consent is needed to participate in a state or national electronic health records system.

☐ ***Express consent***

Express consent is consent that is clearly and unmistakably communicated. Express consent may be given in writing, orally or in any form where the consent is clearly communicated. Wherever practicable, express consent should be sought in writing. If a person gives their express consent orally or by other means such as through a language or sign interpreter, you should document this in your records.

☐ ***Implied consent***

Implied consent is consent that can reasonably be inferred from a person's conduct or actions. However, it may be difficult to demonstrate that a person has genuinely consented, if consent is merely inferred by an organisation. Because of this, it is generally preferable to seek a person's express consent.

If you intend to rely on implied consent, you should be careful not to make assumptions that are not based on fact. For example, it may not be appropriate to infer consent just because a person has not stated their objection to the proposed conduct. The person may not have heard, may not have understood or may have had insufficient information to make an informed decision about the conduct.

Can a person withhold consent?

Where a person will not consent to the use of their information, the refusal must be respected. If you believe that the refusal will cause detriment to the person, you should explain any implications of the refusal.

Are there times when consent is not needed?

The HRIP Act recognises that there are a range of circumstances where the consent of the person is not required in order to lawfully use or disclose their health information. These circumstances are discussed in **Part 2.3** of this handbook. The most important examples include where:

- You are using or disclosing the person's health information for the primary purpose for which it was collected.
- You are using or disclosing the person's information for a directly related secondary purpose, and the person would reasonably expect that use or disclosure.
- You are lawfully authorised or required to use or disclose the person's health information in that way.

Are there times when it is impracticable to seek a person's consent?

Sometimes it will be impracticable for you to seek the person's consent to use or disclose their health information. This may be the case, for example, where you collected the information many years ago and you now seek to use or disclose it for a secondary purpose (such as to a researcher for a research project).

However the fact that seeking consent is inconvenient or would involve some effort or expense is not of itself sufficient to warrant it impracticable. Some examples of where it might be impracticable to seek a person's consent include if:

- the age and / or volume of the information is such that it would be very difficult or even impossible to track down all the individuals involved in order to seek their consent
- there are no current contact details for the individuals in question and there is insufficient information to get up-to-date contact details in order to seek their consent

1.4 CAPACITY

Sometimes people lack the capacity to give consent to, and make decisions about, the collection, use or disclosure of their health information. A person's incapacity may be due to youth, age, mental illness, intellectual disability, dementia, brain injury, illness, accident or disease. For some people, the incapacity may be temporary, while for others it may be permanent.

Where a person lacks capacity to make an informed decision under the HRIP Act, an authorised representative can make decisions on the person's behalf. However the person to whom the information relates should always be involved in the decision to the greatest extent possible.

See section 7 of the *Health Records and Information Privacy Act 2002 (NSW)*
See section 8 of the *Health Records and Information Privacy Act 2002 (NSW)*

How do you assess a person's capacity under the HRIP Act?

☐ ***Test for capacity***

The HRIP Act establishes a test for capacity[19]. The test is that a person lacks capacity to make decisions under the HRIP Act if they:

- are unable to understand the general nature and effect of a particular decision or action under the HRIP Act, or
- cannot communicate their intentions or consent (or refusal of consent) to the decision or action under the HRIP Act.

It is acknowledged that applying this test for capacity involves making difficult judgements and considering complex issues.

☐ ***Capacity depends on the support provided to make a decision***

A person's capacity may depend on whether appropriate support is provided to enable them to exercise their capacity. For example, many people with an intellectual disability are capable of making decisions, if information is communicated in a way that is appropriate to their abilities and usual methods of understanding. If a person has a low level of English language proficiency or is from a culturally diverse background, it is important to provide information in their first language or in a manner that is culturally appropriate so that they can exercise their capacity to the greatest possible extent.

☐ ***A 'bad' decision does not indicate incapacity***

A person may make a decision that you regard as uninformed or misguided, but still have capacity. To have capacity, a person does not need to make what other people might regard as a 'good' or 'right' decision, or even a decision that may be in the person's best interests. A person only needs to understand the general nature and effect of a particular decision or action and be able to communicate their intentions or consent.

When should you deal with an authorised representative?

Where a person lacks the capacity under the HRIP Act to make a decision about their health information, the HRIP Act provides[20] that the following 'authorised representatives' may make the decision on behalf of that person:

- someone who has an enduring power of attorney for the person
- a guardian as defined in the *Guardianship Act 1987*
- a 'person responsible' under section 33A of the *Guardianship Act 1987*
- if the person is a child under the age of 18, a person who has parental responsibility for them
- any other person who is authorised by law to act for or represent the person (including an executor or administrator of a deceased estate).

Young people and capacity

Young people have the right to privacy for their health information and to make their own decisions regarding this privacy where they have the capacity to do so. Parents and guardians do not have automatic access to the health information relating to a young person in their care, and you should not automatically disclose a young person's health information to a parent or guardian.

The HRIP Act does not specify at what age a person has the capacity to give consent for the collection, use or disclosure of their health information. This means that you should assess the young person's capacity in accordance with the general test for capacity set out above. Assessment must be done on a case-by-case basis.

Where the young person is assessed as lacking capacity under the HRIP Act and is less than 18 years of age, a parent who has parental responsibility for the young person can act as the young person's authorised representative. In these cases you are permitted to discuss the young person's health information with his or her parent(s).

For more information, please see Privacy NSW's 'Best Practice Guide on People with Decision Making Disabilities'

PART 2: YOUR LEGAL OBLIGATIONS UNDER THE HRIP ACT – THE 15 HEALTH PRIVACY PRINCIPLES (HPPs)

2.1 COLLECTING HEALTH INFORMATION

You can collect a person's health information for a lawful purpose that is directly related to your organisation's functions. Only collect the health information that you need in a fair, direct and unobtrusive manner.

Health privacy principles 1-3
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

What is collection?

In very general terms, 'collection' refers to the process by which you come into possession of a person's health information. You collect health information if you gather, acquire or obtain it directly from the person to whom it relates or from another source.

Collection occurs at the point where you first receive the person's health information. Subsequent exchanges of information between staff are referred to as "use", and discussed at **Part 2.3** of this handbook.

❑ ***Unsolicited collection***

For the purposes of the HRIP Act, health information is not collected by an organisation if the receipt of the information by the organisation is unsolicited.[1] The term 'unsolicited' is not defined in the HRIP Act.

However as a best practice tip, Privacy NSW recommends that wherever you receive health information without asking for it and then decide to keep that health information, you should regard this as a collection.

❑ ***Can you collect health information merely by seeing or hearing it?***

It is possible to collect health information purely by seeing or hearing it, and without actually recording it anywhere[2].

Example:

Question:
An auditor reviews an organisation's record management practices by randomly selecting and viewing files (some files contain people's health information). The auditor doesn't actually record the health information contained in the files, nor does the auditor take copies or remove the files from the organisation's premises. Is this a collection of health information?

Answer:
Yes. The auditor has sighted the health information in the course of his/her work, and has therefore collected it. The potential for the auditor to use or disclose the health information to the person's detriment, makes it important for these types of collections to come within the coverage of the HRIP Act.

When can you collect a person's health information?

You can only collect health information for a purpose that is directly related to your organisation's functions or activities. The collection must be necessary for that purpose.

Tip for Compliance:

At the time of collection, think carefully about your organisation's functions and the purpose for which you are collecting the health information. Do you really need the health information in order to carry out your purpose?

Information cannot be collected by unlawful means.

Example:

Health information cannot be collected through recording a conversation without a person's consent, as this would breach laws relating to listening devices in NSW.

Information must be relevant, and accurate. The collection must not be intrusive or excessive.

You must collect only as much health information as is needed to carry out your purpose. The information should be relevant, accurate, up to date, complete and not excessive.

Example:

An organisation's form contains multiple fields to collect much standard information. The form is used for a number of purposes. Often, people may have the impression that they must fill in all the fields, even if this is unnecessary and inappropriate. This would probably be an irrelevant and excessive collection of health information.

The collection of information must not unreasonably intrude on the personal affairs of the person.

Example:

An employee provides a medical certificate to his/her employer for sick leave. The medical certificate states that the employee has undergone surgery. It might be unreasonably intrusive for the employer to demand toknow more details about the employee's operation, before approving the sick leave.

Can you collect health information about a person from someone else?

You should collect health information about a person directly from that person, unless it is unreasonable or impracticable to do so. If it is unreasonable or impracticable, you may collect health information from someone else.

Some examples of when it may be unreasonable or impracticable to collect directly from the person are:

- *If a person is admitted unconscious to an emergency ward you may, as a health service provider, need to ask their relatives for any background health information of relevance to how the person is treated.*
- *If a person lacks the capacity to provide their health information, you may need to collect health information about them from an authorised representative such as a carer or guardian.*
- *In the course of taking the family, social or medical history of a patient, you may collect health information about a person other than your patient, if this is relevant to providing the health service to your patient.*
- *In certain circumstances your organisation may collect health information about a person from another person or organisation rather than directly from the person themselves.*

2.2 NOTIFYING A PERSON WHEN YOU COLLECT THEIR HEALTH INFORMATION

When you collect a person's health information you are required to notify them of certain things. This is the case even when you collect a person's health information from someone else. You must take reasonable steps to ensure that the person is aware of:

- the identity of your organisation and how to contact it
- the purposes for which the information is collected
- any other organisation which is usually provided with the same information
- any law that requires the particular information to be collected
- the fact that they are able to request access to the information
- the main consequences, if any, for the person if all or part of the information is not provided

Health privacy principle 4
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

What and why should you notify the person?

When you collect a person's health information you must notify the person of the information set out in the box above. This promotes transparency and shared expectations between the person and your organisation. It allows you to explain why you are collecting the person's health information and who will see it. It allows the person to make informed decisions on the basis of this information.

❑ ***Notifying patients of information sharing amongst the 'treating team'***

It is common in the Australian health system for practitioners to adopt a multi-disciplinary approach to health care. The treating team will often work together to treat the patient and share any information about the patient regarded as relevant to the treatment.

It is Privacy NSW's experience that privacy complaints can occur where patients have not been told that their information will be shared amongst the treating team, and do not expect it.

As discussed in **Part 1.3** of this handbook, notifying a person of how their health information will be handled is not the same as seeking their consent to do those things. However, by notifying the person of the team-based approach to treatment, and of the likelihood that their information will be shared amongst members of the 'treating team', you are reducing the risk of misunderstandings and subsequent privacy complaints.

If you have notified the person that their information could be used by or disclosed to other health practitioners in this way, there is a persuasive argument that such a use or disclosure would be within the person's 'reasonable expectations'. This would put you in a better position to rely on the 'directly related secondary purpose within the reasonable expectations of the individual' exemption as regards use and disclosure of health information in HPPs 10(1)(b) and 11(1)(b). Please refer to **Part 2.3** of this handbook for more information.[3]

Tip for Compliance:

Your aim here should be to ensure that your patient's expectations for the use and disclosure of their health information align with yours and actual practice. If unsure, you should check with the patient.

When should you notify the person?

You must notify the person of the required information at or before the time of collection. If that is not practicable, you must notify them as soon as practicable after that time.

Example:

Where a patient presents to the hospital's emergency department, there simply may not be time, or the person may not be in a fit state, to comprehend the information. In such circumstances, you should notify them of the required information as soon as it is practical afterwards.

How should you notify the person?

You must take steps that are reasonable in the circumstances to notify the person of the required information. This can be done in a variety of ways, including verbally or by written communication, or a combination of the two. From a risk management point of view, however, it is easier to demonstrate compliance if the notification was in writing.

Tip for Compliance:

Where your organisation collects health information by way of a form, your obligations under HPP 4(1) could be satisfied by a prominent and easy to read statement on that form. For health service providers, one useful way to provide the information is via a notice clearly displayed in the admissions or patient waiting area of the organisation, or by pamphlets and brochures.

Sometimes you may need to notify an authorised representative instead

If you reasonably believe that the person is incapable of understanding the general nature of these points, you may notify the person's authorised representative instead. For more information on who is an authorised representative and when they should be contacted, please see Part 1.4 of this handbook.

Best Practice Tip:

Where you need to deal with an authorised representative you should still, where practicable, explain the points to the person to whom the information relates in a way that is appropriate to their level of understanding. This is to enable the person to be involved in the notification process to the greatest extent possible.

In certain circumstances you are not required to notify the person

In some circumstances, notifying the person is not necessary or appropriate. You are not required to notify the person if:

- the person has expressly consented to not being notified
- your organisation is lawfully authorised or required not to notify the person
- not notifying the person is permitted or is necessarily implied or reasonably contemplated under an Act or any other law
- notifying the person would prejudice their interests
- the information has been collected for law enforcement purposes
- your organisation is an investigative agency[4] and notifying the person might detrimentally affect or prevent the proper exercise of your organisation's complaint handling or investigative functions

Notifying a person when you have collected health information about them from someone else

You are required to notify a person of the required information even when you have collected health information about them from someone else. The exceptions are where:

- you collect health information about the person from someone else and notifying the person would pose a serious threat to the life or health of any person or
- you comply with the NSW Privacy Commissioner's statutory guidelines.

❑ ***Statutory guidelines on notifying a person when you have collected health information about them from someone else***

The NSW Privacy Commissioner's statutory guidelines provide that you do not have to notify a person when you have collected health information about them from someone in circumstances where:

- You collected information from the third party because it was unreasonable or impracticable to collect directly from the person and it would also be unreasonable or impracticable to notify the person;
- The information was collected in the process of recording a family, social or medical history and this was necessary to provide health services to the client;

- The information was collected from an authorised representative, because you believe the person was incapable of understanding the nature of the information required;
- The information was initially collected by another organisation and there are reasonable grounds to believe that the person has already been informed of the required information by the first organisation.

You should read the full requirements of the statutory guidelines, if you wish to rely on them. The statutory guidelines on notifying a person when you have collected health information about them from someone else, are published on the Privacy NSW website.

2.3 USING AND DISCLOSING HEALTH INFORMATION

In general, you may only use and disclose health information about a person for the primary purpose for which the information was collected.

However in certain circumstances (outlined below), health information may be used and disclosed for a secondary purpose other than the primary purpose for which it was collected.

Health privacy principles 10 & 11

See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

What is use and disclosure?

In general terms:

- 'use' refers to the communication or handling of health information within an organisation.
- 'disclosure' refers to the communication or transfer of information outside an organisation.

Sometimes, the distinction between 'use' and 'disclosure' is not clearly defined. However, in practice this is less important. Under the HRIP Act, the rules about how you can use health information (see **HPP 10**) and disclose health information (see **HPP 11**) are almost identical.

Use and disclose health information only for the primary purpose for which it was collected

❑ ***Use and disclosure for a primary purpose***

Generally, you may use and disclose health information about a person only for the primary purpose for which the information was collected. The primary purpose is the main or dominant reason for which the information was collected and is strictly necessary to discharge your organisation's functions and activities. Other purposes are 'secondary'.

Example 1:

If a person is admitted to hospital for day surgery, the primary purpose for collecting their health information at admission is to provide them with the day surgery. The person's information may be used by those involved in providing the day surgery, including anaesthetists, nurses and pathologists, as the information is being used for the same primary purpose for which it was collected. Such uses may occur without obtaining the further consent of the person.

Example 2:

An insurance company asks a person to fill in a form outlining details of the injuries that they sustained in an accident in order to process their insurance claim. The information can be used by the insurance company's claims manager in order to assess and process the claim, because that is the primary purpose for which the information was collected.

- ***Use and disclosure for a secondary purpose***

In certain circumstances health information may be used and disclosed for a secondary purpose other than the primary purpose for which it was collected.

Secondary purposes include some that are considered 'directly related' to the primary purpose and others which are more remote.

Example:

Some months after a patient's discharge, the oncology unit proposes to conduct a fundraising drive and wants to use the information from medical records to target recent admissions. As fundraising was not the primary purpose for which this information was collected, the use for this secondary purpose could only proceed if it comes within one of the permitted exemptions below.

Use and disclosure for secondary purposes – some permitted exemptions

The secondary purposes for which you are permitted to use or disclose health information are outlined below.

- ***With the consent of the person***

Health privacy principles 10(1)(a) &11(1)(a)
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

You may use or disclose a person's health information for almost any secondary purpose if you have the person's consent. The concept of consent is explained in more detail in **Part 1.3** of this handbook.

Example:

An organisation assists those who are frail, aged, or have a disability, to remain at home rather than in institutional care by undertaking modifications to their home (such as installing handrails and ramps). The organisation collects health information in order to do this.

A wheelchair manufacturer approaches the organisation asking it to disclose the contact details of any immobile clients. The manufacturer wants to send the clients marketing material about a new wheelchair product. In this context the contact names and details alone would be 'health information' and covered by the HRIP Act, because they say something about the physical health of the person. Provided the organisation obtains the consent of the clients, it can disclose their health information for this secondary purpose.

- ***Directly related secondary purpose within the reasonable expectations of the person***

Health privacy principles 10(1)(b) & 11(1)(b)
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

You may use or disclose health information without the consent of the person when there is:

- a directly related secondary purpose that is
- within the reasonable expectations of the person.

Example:

If the health information is collected in order to provide a health service to the person, the use of the information to provide a further health service to the person is a secondary purpose directly related to the primary purpose. This should usually be within the reasonable expectations of the person. The further consent of the person is not required.

In deciding what the reasonable expectations of the person are, you should look at what the ordinary person in the street, who has no special knowledge of the organisation or industry, would expect.

Examples of uses and disclosures that may fall within this 'direct relation' exemption include:

- Using the information to provide ongoing care to patients, or an ongoing service to clients
- Disclosing information to another person or organisation involved in the ongoing care of the patient, or the ongoing service to the client
- Investigating and managing adverse incidents or complaints about care or patient safety
- Sending reminders to a person where the person receives a service on a regular basis or requires a follow up service
- Disclosing information to a debt collection agency to follow up an overdue payment
- Using information for quality assurance activities carried out by the organisation such as monitoring, evaluating, auditing the provision of a particular product or service the organisation has or is providing the person
- Disclosing information to an auditor or quality assessor for the purposes of monitoring, evaluating, auditing the provision of a particular product or service the organisation has provided or is providing to the person (as long as the individual reviewing the records understands and agrees to be bound by the HPPs or their equivalent)
- Managing a legal claim made by the person

Best Practice Tip:

You should make the person aware that these activities are carried out as part of the normal functioning of your organisation. If you make it clear to the person that their information may be used or disclosed for these purposes, there is a more persuasive argument that the person would 'reasonably expect' you to use or disclose their information in these ways.

❑ *Serious threat to health or welfare*

Health privacy principles 10(1)(c) & 11(1)(c)
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

You may use or disclose health information without the consent of the person to lessen or prevent:

- a serious and imminent threat to the life health or safety of any person, or
- a serious threat to public health or public safety

Such disclosure or use must be approached with caution. Situations of serious and imminent threat will be a relatively uncommon occurrence. You must reasonably believe that the use or disclosure of the health information is necessary to prevent that threat. You need to carefully assess the level of risk before acting.

Example:

A person attends a counselling session in a highly agitated state, and expresses an intention to return home and inflict serious harm on their partner. The client has a history of domestic violence and has faced previous assault charges. The counsellor would have reasonable grounds to believe that the client's partner was at serious and imminent risk and could therefore appropriately disclose the information, in order to address this risk.

❑ *Management of health services, training or research*

Health privacy principles 10(1)(d), 11(1)(d), 10(1)(e), 11(1)(e), 10(1)(f), 11(1)(f)
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

You may use or disclose health information without the consent of the person for:

- the funding, management, planning or evaluation of health services;
- training;
- research, or the compilation or analysis of statistics, in the public interest.

However these exemptions only apply where you have satisfied the following threshold issues:

- the use or disclosure is reasonably necessary for the purpose; and
- you have taken reasonable steps to de-identify the information, or the purpose of the activity cannot be served by using or disclosing de-identified information; and it is impracticable to seek the consent of the person to the use or disclosure; and
- if the information could reasonably be expected to identify people, the information is not going to be published in a generally available publication; and
- the use or disclosure of the information is in accordance with the NSW Privacy Commissioner's statutory guidelines.

Tip for Compliance:

Before relying on the management of health services, training or research exemptions, you should consider whether you may be able to use or disclose:

- *with the consent of the person under the 'consent' exemption; or*
- *under the 'directly related secondary purpose within the reasonable expectations of the person's exemption.*

Is the use or disclosure reasonably necessary?

When deciding whether the use or disclosure is reasonably necessary, consider to what degree the health information is needed for the activity. For example sometimes the activity may be just as effectively undertaken using hypothetical case studies, or simulated situations.

Example:

Question: A researcher proposes to assess the effectiveness of a software package for use by psychologists. The researcher wants to do this by monitoring how the psychologist enters information into the system during sessions with clients (eg. which icons the psychologist uses, how many keystrokes the psychologist takes to get to particular screens). The researcher proposes to monitor this remotely (that is, the researcher will not be present in the session). However the researcher will be able to view all of the client's information as it is entered into the system. Is such a disclosure reasonably necessary?

Answer:
No. The disclosure of the client's health information to the researcher is not reasonably necessary here. Simulated situations should suffice to achieve the purpose, or the consent of the client should be sought.

The purpose cannot be served by de-identified information

If the activity could be undertaken using or disclosing de-identified information, then you should proceed this way. This may involve converting 'identifiable' information (information that allows the identification of a specific person) into 'de-identified' information. De-identified information is information from which identifiers have been permanently removed, or where identifiers have never been included. De-identified information cannot be re-identified.

However sometimes de-identified information cannot achieve the purpose of the activity. This could be, for example, where an activity involves linking information about individuals from two or more sources and you need identified information to correctly link records from each data source.

It is impracticable to seek the person's consent

The considerations when deciding whether it is impracticable to seek the person's consent are explained in **Part 1.3** of this handbook.

Reasonable steps to de-identify the information

When de-identifying information, you should consider the capacity of the person or organisation receiving the information to re-identify it or re-link it to identifiable information. Removing the name and address may not always be enough, particularly if there are unusual features in the case, a small population, or there is a discussion of a rare clinical condition. Reasonable steps to de-identify information might also include removing other features, such as date of birth, ethnic background and diagnosis that could otherwise allow an individual to be identified in certain circumstances.

The information will not be published in a generally available publication

A 'generally available publication' is defined in section 4 of the HRIP Act to mean a publication that is generally available to members of the public, either in paper or electronic form.

The NSW Privacy Commissioner's statutory guidelines

The NSW Privacy Commissioner has issued statutory guidelines that set out the last set of conditions under which health information may be used or disclosed for management, research and training. The statutory guidelines form part of the law. You must comply with them if you are seeking to rely on the management, research or training exemptions.

The statutory guidelines on the management of health services require that you ask a series of questions about the proposed management activity before using or disclosing. If any of the questions are answered in the affirmative, the management of the health services activity must be approved by a Human Research Ethics Committee before you can use or disclose. To view the statutory guidelines on the management of health services please see the Privacy NSW website at: **www.lawlink.nsw.gov.au/privacynsw**

The statutory guidelines on research are consistent with, and mirror, the guidelines developed by the National Health & Medical Research Council under sections 95 and 95A of the Federal *Privacy Act 1988.* The statutory guidelines on research require that a Human Research Ethics Committee approve the research proposal before you can use or disclose. The statutory guidelines on research are available online at the Privacy NSW website at: **www.lawlink.nsw.gov.au/privacynsw**

The statutory guidelines on training require that every employee or person working with the organisation, who will be trained or who will access the health information during the training process, signs an undertaking stating that they have been made aware of the requirements of the HPPs in the HRIP Act and that they understand they are required to comply with them. The statutory guidelines on training also set requirements for managing such training. To view the statutory guidelines on training please see the Privacy NSW website at: **www.lawlink.nsw.gov.au/privacynsw**

- ❑ ***Find missing person***

Health privacy principles 10(1)(g) & 11(1)(h)
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

You may use or disclose health information without the consent of the person if the information is to be used by a law enforcement agency to find a missing person. This exemption only applies if the person has been reported as missing.

Section 4 of the HRIP Act defines 'law enforcement agency' to mean any of the following:

- NSW Police or the police force of another State or Territory
- Australian Federal Police
- NSW Crime Commission
- Australian Crime Commission
- Director of Public Prosecutions of NSW or of another State or Territory or of the Commonwealth
- Department of Corrective Services
- Department of Juvenile Justice

Example:

The police have received a report from a family that their 17 year old son is missing. The boy has a chronic condition requiring regular treatment in hospital. The police request information from a hospital to ascertain if he has been admitted as a result of a failure to take his medication. The hospital would be entitled to provide this information under the 'find missing person' exemption.

❑ *Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline*

Health privacy principles 10(1)(h) & 11(1)(i)
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

Organisations may use or disclose health information without the consent of the person where the organisation has reasonable grounds to suspect that:

- unlawful activity has been or may be engaged in, or
- a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under a health registration Act, or conduct that may be grounds for disciplinary action.

The use or disclosure must be a necessary part of investigating or reporting suspected unlawful activity.

This exemption recognises that organisations have a legitimate function in conducting internal investigations and reporting suspected unlawful activity.

Example:

Staff members have raised concern about a colleague's conduct towards female clients. They have witnessed the colleague being sexually inappropriate towards female clients and using derogatory terms to describe females in his file notes.

In order to conduct an internal investigation, the organisation may need to review client files (some containing health information). The organisation may rely on the 'suspected unlawful activity' exemption to use health information in this way.

❑ *Law enforcement*

Health privacy principles 10(1)(i) & 11(1)(j)
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

You may use or disclose health information without the consent of the person if:

- this is reasonably necessary for a law enforcement agency to carry out its functions, and
- there are reasonable grounds to believe that an offence may have been committed.

The list of law enforcement agencies is set out under the 'Find missing person' exemption above.

This exemption does not **require** you to provide information to the law enforcement agency. In the absence of a warrant or other legal authority, you are entitled not to disclose the information. This exemption is also not intended to **override** any duties of confidentiality that you may owe (for example between a medical practitioner and a patient). This exemption exists to **permit** you to lawfully co-operate with agencies performing law enforcement functions where appropriate.

Tip for Compliance 1:

In deciding whether to disclose to a law enforcement agency, you should consider:

- *the seriousness of the offence being investigated (an investigation into an alleged murder might justify disclosure more than an investigation into property theft)*
- *whether the circumstances indicate a serious and imminent threat to the life, health or safety of any person (such circumstances might better justify a disclosure)*
- *your relevant professional and ethical obligations*
- *how to best balance the protection of the person's privacy as against the investigation and enforcement of the law.*

Tip for Compliance 2:

If you decide to disclose to the law enforcement agency, you should:

- *limit your disclosure to information that is relevant and necessary for their purpose (generally, the information disclosed should be limited to confirmation of identity and address)*
- *obtain and document proof that the person seeking the information is a representative of the appropriate law enforcement agency*
- *keep a written record that you have disclosed.*

Example:

Question: The police are investigating a series of sexual assaults committed by a serial rapist. The offender has indicated that he will rape again. The most recent victim has described very specific injuries that she inflicted on the offender during her attack. Can a doctor who has recently treated someone with these specific injuries, and believes that the patient may be the offender, disclose information to the police?

Answer: If the injury is so distinct that it is unlikely that anyone but the offender would have sustained the injury, disclosure may be justified under this 'law enforcement' exemption[5].

- ***Investigative agencies***

Health privacy principles 10(1)(j) & 11(1)(k)
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

You may use or disclose health information without the consent of the person where this is reasonably necessary for investigative agencies to exercise their complaint handling or investigative functions.

Section 4 of the HRIP Act defines 'investigative agency' to mean any of the following:

- Ombudsman's Office
- Independent Commission Against Corruption
- Police Integrity Commission, the Inspector of the Police Integrity Commission and any staff of the Inspector
- Community Services Commission
- Health Care Complaints Commission
- Office of the Legal Services Commissioner

Where the public sector agency is not an investigative agency but is handling a matter that has been referred from, or could be referred to, an investigative agency, this exemption also applies[6].

Tip for Compliance:

As with the 'law enforcement' exemption, in the absence of a warrant or other legal authority you are permitted, but not required, to disclose to an investigative agency. In deciding whether to disclose to an investigative agency you should apply the same considerations as set out under the 'law enforcement' exemption above.

❑ *Prescribed circumstances*

Health privacy principles 10(1)(k) and 11(1)(l)
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

The HRIP Act permits you to use or disclose health information as prescribed by regulations made by the Governor[7]. To date, no regulations have been made for the purposes of this paragraph.

❑ *Lawfully authorised or required, or permitted under another law*

Health privacy principles 10(2) and 11(2)
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

You may use or disclose health information without the consent of the person, where you are lawfully authorised or required, or permitted under another law to do so. The HRIP Act does not override other legislation.

Example:

You may be required to:

- *disclose health information to the Department of Community Services (DOCS) where a child or young person is at risk of harm under section 23 of the Children and Young Persons (Care and Protection Act)*
- *disclose health information involving notifiable diseases pursuant to the Public Health Act 1991*
- *disclose health information pursuant to search warrants or subpoenas.*

❑ *Disclosures on compassionate grounds*

Health privacy principle 11(1)(g)
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

You may disclose health information without the consent of the person to an immediate family member for compassionate reasons where:

- the person is incapable of giving consent, and
- the disclosure is not contrary to any wish expressed by the person (and not withdrawn) of which you are aware or could reasonably make yourself aware, and
- if the immediate family member is under the age of 18 years, you reasonably believe that they have sufficient maturity in the circumstances to receive the information, and
- the disclosure is limited to the extent reasonable for those compassionate reasons.

An 'immediate family member'[8] means a:

- parent, child or sibling of the person, or
- spouse of the person, or
- member of the person's household who is a relative of the person, or
- person nominated to an organisation by the person as someone to whom health information relating to the person may be disclosed

Example:

A patient is admitted to the emergency ward of a hospital unconscious as the result of a car accident. This exemption permits the hospital to contact the patient's next of kin to advise them of the patient's admission.

2.4 RETENTION AND SECURITY

You must take reasonable measures to protect the health information you hold (or that someone holds on your behalf) from misuse and loss, and from unauthorised access, use, modification or disclosure.

You must keep health information for no longer than is necessary for the purpose of its lawful use (however noting minimum retention periods prescribed by law).

Dispose of health information securely and in accordance with any retention and disposal requirements to which you are bound.

Health privacy principle 5
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

If you are in the private sector you are also governed by Part 4, Division 2

What security safeguards should you take to protect health information?

You must take such security safeguards as are reasonable in the circumstances to protect the security of the health information. If health information is not held and managed securely, the risks of privacy breaches (intentional and unintentional) are increased.

Some reasonable *physical* safeguards might include:

- Locking filing cabinets and unattended storage areas
- Physically securing the areas in which the health information is stored
- Not storing health information in public areas
- Positioning computer terminals and fax machines so that they cannot be seen or accessed by unauthorised people or members of the public.

Some reasonable *technical* safeguards might include:

- Using passwords to restrict computer access, and requiring regular changes to passwords
- Establishing different access levels so that not all staff can view all information
- Ensuring information is transferred securely (for example, not transmitting health information via non-secure email)
- Using electronic audit trails
- Installing virus protections and firewalls.

Some reasonable *administrative* safeguards might include:

- Introducing appropriate policies and procedures to address information security
- Training staff on those policies and procedures.

How long are you required to retain health records?

You are required to destroy or permanently de-identify health information once it is no longer needed for further uses or disclosures authorised by the HRIP Act. However this requirement is not absolute. If other legislation requires you to retain records for a minimum period, then this must be followed.

❑ ***Public sector agencies***

Public sector agencies are subject to the requirements of the *State Records Act 1998 (NSW).* That Act has extensive provisions as to the minimum length of time that public records should be retained. You should go to **www.records.nsw.gov.au** for further information.

❑ ***Private sector health service providers***

See Part 4, section 25(1) of the *Health Records and Information Privacy Act 2002 (NSW)*

Private sector health service providers must retain health information relating to the person as follows:

- In the case of health information collected while the person was an adult – for 7 years from the last occasion on which you provided the person with a health service
- In the case of health information collected while the person was under the age of 18 years – until the person has attained the age of 25 years.

Disposing of health information, or transferring health information to another organisation

You are required to dispose of health information securely.

❑ ***Private sector health service providers***

See Part 4, section 25(2)-(4) of the *Health Records and Information Privacy Act 2002 (NSW)*

When private sector health service providers delete or dispose of a person's health information they must keep a record of:

- the name of the person
- the period covered by the health information
- the date on which it was deleted or disposed of.

When private sector health service providers transfer a person's health information to another organisation (and do not continue to hold a record of that information) they must keep a record of the name and address of the organisation to which they transferred the health information.

2.5 ACCESS AND AMENDMENT

People have a right to request access to the health information that you hold about them. You should give a person access to their health information if they ask for it, unless particular circumstances apply.

People have a right to request amendments to the health information that you hold about them, where they believe the information is inaccurate, irrelevant or misleading. Where appropriate, you should make these amendments.

Health privacy principles 6, 7 & 8
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

If you are in the private sector you are also governed by Part 4, Divisions 3 & 4

Obligation to be transparent about the health information you hold

Health privacy principle 6
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

Before people can seek to access or amend their health information, they need to know who holds it. You are required to take reasonable steps to enable any person to find out what health information you hold about them, why, and how they can seek access to it.

Best Practice Tip:

Your organisation's privacy policy is one way of being transparent about the health information that you hold as required by HPP 6.

How can a person make a request for access or amendment?

The rights of access and amendment are triggered by a request from the person to whom the health information relates. A person should follow a certain format when making a request for access and / or amendment under the HRIP Act. The rules about the format of a request differ depending on whether the request is to a public sector or private sector organisation.

- ***Requests to public sector agencies***

Where a person seeks to access or amend their health information held by an organisation in the public sector, the HRIP Act does not require the person's request to be in writing.

Example:

During a consultation at her public hospital, Jane asks for a copy of her latest test results. The hospital can satisfy this request for access by simply providing a copy of the information at the time.

If the request is not as straightforward as the example above, you may prefer to ask the person to put their request in writing. A written request allows clarity about the information for which access or amendment is sought and provides a written record of the request on file. There are no rules under the HRIP Act about what information a request to a public sector organisation should contain.

Note that access to health information held by public sector agencies may also be available under the *Freedom of Information Act 1989* or the *State Records Act 1998.* If people are seeking access to their health information under those Acts, they should comply with the requirements set out under those Acts.

Example:

Question: What is the difference between access under the Freedom of Information Act 1989 and access under the HRIP Act?

*Answer: The FOI Act allows **any** person to apply for access to **any** documents held by the government. It is designed to facilitate open and transparent Government. The HRIP Act allows a person to apply for access to their **own** health information (not limited to documents).*

❑ ***Requests to the private sector***

See **Part 4, section 26** of the *Health Records and Information Privacy Act 2002 (NSW)*

Where a person seeks to access or amend their health information held by a private sector organisation, the HRIP Act requires the person's request to:

- be in writing, and
- state the name and address of the person making the request, and
- identify the health information they wish to access or amend

If the request is for access, the person must specify the form in which they require the information to be provided.

If the request is for amendment on the grounds of incomplete or out of date health information, the request must contain the information the person claims is necessary to complete the health information or bring it up to date.

NB: Difference with Federal Privacy Act:

Under the Federal Privacy Act, *it is not a legal requirement that requests be made in writing.*

Tip for Compliance:

Even if the person's request is not in the form set out above, you may still decide to provide the person with the access or amendment that they have requested. The HRIP Act is not intended to prevent or discourage you from providing a person with access or amendment in other circumstances. For example if someone from a non-English speaking background has difficulties putting their request in writing, you may decide to grant them with access on the basis of a verbal request.

Fees and charges

Privacy NSW encourages organisations to provide access and amendment without charge.

However you are permitted to charge a fee to cover the administrative costs of providing access (e.g. for copying or printing records). The fee should not be excessive, nor should it discourage people from seeking access to their health information[9].

Can a request for access or amendment be made by someone other than the person to whom the information relates?

Where a person lacks capacity to make a request about their own health information, an authorised representative may make a request on the person's behalf. See **Part 1.4** of this handbook for more on capacity and authorised representatives.

A person can also consent for someone else to access health information on their behalf. For example a person can consent to, or authorise any third party, such as a relative, interpreter, medical practitioner, legal representative, employer or insurer, to have access to their health information. Members of parliament making representations on behalf of a constituent are also required to have the person's authorisation. It is important to check how specific the authority is, and the exact scope of the authority that the person has provided. You must ensure that such authorisations are in writing and clearly state the name of person who is authorised to have access.

For information on circumstances where a parent wants to see their child's health information, please see **Part 1.4** of this handbook.

Check identity of person making request

You should check the identity of the person making the request and be satisfied that the person is who they say they are.

How much time do you have to respond to a request for access or amendment?

- ❑ ***Public sector***

Health privacy principle 7
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

If you are in the public sector, the HRIP Act requires you to respond to a request for access 'without excessive delay'. Responses to requests for amendment should also be responded to without excessive delay.

❑ ***Private sector***

See **Part 4, Section 29** of the *Health Records and Information Privacy Act 2002 (NSW)*

You can refuse a person access to their health information only if:

- providing access would pose a serious threat to the life or health of any person *(for example, where there is a risk that the information may cause the person significant distress so as to result in them harming themselves or another)*
- providing access would have an unreasonable impact on the privacy of other people (however, where a person's health record contains information about someone else, you can prevent an unreasonable impact on that other person's privacy by removing that other person's identifying details before releasing the information)
- the information relates to legal proceedings (existing or anticipated) between your organisation and the person, and the information is subject to legal professional privilege or would not be accessible by the process of discovery
- providing access would reveal your organisation's intentions in relation to negotiations with the person in such a way as to expose you to disadvantage (*for example, regarding the settlement of a negligence claim)*
- providing access would be unlawful
- denying access is required or authorised under another law
- providing access would be likely to prejudice an investigation of possible unlawful activity
- you have been asked by a law enforcement agency performing a lawful security function not to provide access, as it would be likely to cause damage to the security of Australia
- the request for access is one that has been made unsuccessfully on at least one previous occasion and there are no reasonable grounds for making the request again
- the person has already been provided with access to their information under the HRIP Act and is making an unreasonable repeated request, for access to the same information, in the same manner.

If you decide to refuse access, you must provide a written reason for the refusal. The reason must be provided for under the HRIP Act. In other words, the refusal must be for one of the reasons listed above. Access may be refused to a part of the information to which a request relates, but provided to the remainder of the information.

❑ ***Access refused because of serious threat to person – use of intermediary***

See **Part 4, section 30** of the *Health Records and Information Privacy Act 2002 (NSW)*

Where a private sector organisation refuses to provide the person with access to their health information on the grounds that providing access would pose a serious threat to their life or health, the notice of refusal must:

- advise the person that he or she may nominate a medical practitioner to be given access to the health information instead, and
- advise the person that any nomination must be made within 21 days after receipt of the notice of refusal.

Access must then be provided to the nominated medical practitioner within 21 days of receiving the person's nomination.

Access: in what form should you provide it?

Access may be provided in a number of different ways. You may decide to grant the person access by:

- giving the person a copy of the health information
- providing a reasonable opportunity for the person to inspect the health information, take notes on its contents and talk through the contents with an appropriate staff member if required
- allowing the person to listen to or view the contents of an audio or visual recording
- giving the person a print-out of the information if it is stored electronically, or giving them an electronic copy of the information.

❑ ***Private sector***

For private sector organisations, if the person requests access to be provided in a particular form (for example, they request to receive a paper copy of their health information), then you should generally provide access in that form. You may only refuse to provide access in that form, if it would:

- place unreasonable demands on your organisation's resources
- be detrimental to the preservation of the information
- involve an infringement of copyright.

In these cases, you should provide access in another convenient form.

Amendment: when should you amend health information?

In response to a request for amendment, you may amend (by way of corrections, deletions or additions) the health information to ensure:

- the information is accurate
- the information is relevant, up to date, complete and not misleading, taking into account the purpose for which the information is collected and used.

The HRIP Act states that amendments can be made by way of deletions. However, for legal and medical reasons, Privacy NSW acknowledges that it is generally advisable not to permanently delete the information.

Some requests for amendment will be easy to deal with, for example where a person requests changes to their address details. In these cases you should make such amendments via your usual process, as long as you are satisfied of the identity of the person.

Other requests for amendment will be more difficult to deal with, for example where a person challenges a medical opinion, evaluation or diagnosis.

Amendment: on what grounds can you refuse a request?

See **HPP 8 in Schedule 1, and Part 4 section 34,** of the *Health Records and Information Privacy Act 2002 (NSW)*

You can refuse to amend the person's health information if you are satisfied that:

- the health information is not incomplete, incorrect, irrelevant, out of date or misleading, or
- the request contains information that is incorrect or misleading.

❑ ***Public sector***

If you are not prepared to make the amendment requested, the person can ask you to attach to the record their statement requesting the amendment. You must take reasonable steps to do this.

❑ ***Private sector***

See **Part 4, section 34 and 35** of the *Health Records and Information Privacy Act 2002 (NSW)*

If you are not prepared to make the amendment requested, you must give the person a written reason for the refusal. The person can then ask you (by notice in writing) to add a notation to the health information specifying their claims.

2.6 ACCURACY

> You must take reasonable steps before using health information to ensure that it is relevant, accurate, up to date, complete and not misleading.

You must take reasonable steps before using health information to ensure that it is relevant, accurate, up to date, complete and not misleading.

Health privacy principle 9
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

What are reasonable steps to ensure accuracy?

When collecting health information, you understandably rely on the person providing it to give you information that is relevant, accurate, up to date and not misleading.

It would be burdensome for you to have to continually check and recheck the accuracy of all the data you hold and the HRIP Act does not require this. However, you are required to take reasonable steps to ensure the quality and integrity of your data before using it.

The term ‘reasonable steps’ is not defined in the HRIP Act. However some factors you might like to consider when determining reasonable steps in the circumstances include:

- how recently the information was collected (if it was collected recently, then there may be no need to recheck it now)
- the reliability of the source providing the information (information from an unreliable source should be checked before it is used)
- the likelihood that the information is accurate, up to date and not misleading (the lesser the likelihood, the greater reason to check)
- what you are proposing to use the information for (for example, if you are using it to make a decision about the person’s future health care, it is important that you take steps to ensure the information is accurate).

2.7 IDENTIFERS

You can only assign an identifier to a person where this is reasonably necessary to carry out your organisation's functions efficiently.

Private sector organisations are prohibited from adopting, using or disclosing an identifier assigned by a government agency, except in prescribed circumstances.

Health privacy principle 12
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

What is an identifer?

An identifier is defined in section 4 of the HRIP Act to mean something (usually a number) that an organisation assigns to a person in order to uniquely identify that person. The identifier will have either been created, adopted, used or disclosed in conjunction with or in relation to the person's health information. A person's name is not an identifier.

Example:

The Medical Records Number (MRN) and the Unique Patient Identifier (UPI) are identifiers in the NSW public health system. The Medicare number is an identifier issued by an Australian government agency.

Identifiers bring important benefits for efficient record management. However they also pose privacy risks and can lead to large quantities of data about a person, from different sources, being data-matched and amalgamated into a single source. Although identifiers do not contain a person's name, they are designed to be unique to a particular person and hence will be classified as health information and subject to the HRIP Act.

Prohibitions regarding the private sector and identifiers

A private sector organisation may only adopt a public sector agency identifier as its own where:

- person concerned has consented to this, or
- the use or disclosure of the identifier is required or authorised by or under law.

Example:

An insurance company could not adopt the UPI as its own identifier unless one of the above two conditions has been met.

A private sector organisation may only use or disclose a public sector agency identifier in certain circumstances. See **HPP 12(3)** & **(4)** for a full list of permissible circumstances.

2.8 ANONYMITY

Wherever it is lawful and practicable, you must give people the opportunity to remain anonymous when entering into transactions with, or receiving health services from, your organisation.

Health privacy principle 13
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

Provide a service anonymously where this is lawful and practicable

Sometimes people may wish to remain anonymous or use an alias when dealing with organisations. This may be the case where they are using counselling services, or attending sexual health clinics. They may have other reasons for not wishing to identify themselves, for example, to avoid being targeted for direct marketing, or to avoid being located by an abusive partner. You should permit the person to remain anonymous wherever this is lawful and practicable.

When is anonymity unlawful?

In some cases it will be unlawful to transact business with the person anonymously. This is usually because there is a legal requirement stating that you must collect identifying information from the person. For example:

- when prescribing a restricted drug, you are legally required to provide the name of the person who will receive the drug
- where a person has been diagnosed with certain medical conditions listed as "scheduled medical conditions" under the ***Public Health Act** 1911 (NSW)*, the medical practitioner is required to record certain details, including identity, to allow the matter to be reported to the Department of Health.
- where significant cash transactions take place, the law requires the parties to a transaction to be identified.

When is anonymity impracticable?

In some cases it will be impracticable to transact with the person anonymously. For example:

- where ongoing health care is required and the service requires a follow-up – if the person does not provide details to allow this, their ongoing health care may be compromised
- where a transaction cannot be carried out without providing identifying information, such as in credit card transactions or payments by cheque.

2.9 TRANSFERRING HEALTH INFORMATION OUT OF NSW

Before transferring health information out of New South Wales, make sure the recipient is subject to substantially similar privacy standards or laws.

If equivalent privacy protections do not exist, then you can only transfer the health information out of NSW under certain circumstances (outlined below).

Remember that in transferring health information out of NSW, you will also need to comply with the rules about use and disclosure contained in health privacy principles 10 and 11.

Health privacy principle 14
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

When can you transfer health information out of NSW?

You can transfer health information out of NSW in the following circumstances:

- ❑ ***Recipient subject to substantially similar privacy standards or laws***

You reasonably believe that the recipient is subject to a law, binding scheme or contract that imposes substantially similar obligations to those imposed by the HPPs.

- ❑ ***Consent***

The person has consented to the transfer.

- ❑ ***Contractual obligation***

The transfer is necessary for the performance of a contract between your organisation and the person.

- ❑ ***Benefit to the person***

The transfer is for the benefit of the person, and it is impracticable to obtain their consent, and, if it were practicable to obtain such consent, the person would likely give it.

- ❑ ***Serious threat to health or welfare***

The transfer is reasonably believed to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety to any person, or a serious threat to public health or public safety. See **Part 2.3** of this handbook for more information.

- ❑ ***Reasonable steps***

You have taken reasonable steps to ensure that the health information you transfer will not be held, used or disclosed by the recipient inconsistently with the HPPs.

- ❑ ***Lawful authorisation***

The transfer is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

2.10 LINKAGE OF HEALTH RECORDS AT STATE OR NATIONAL LEVEL

You must obtain the express consent of the person, before including their health information in a state or national electronic health records scheme. Participation is opt-in, not opt-out.

Health privacy principle 15
See Schedule 1 of the *Health Records and Information Privacy Act 2002 (NSW)*

When does this health privacy principle apply?

HPP 15 does not apply to all electronic storage and linkage of health records. It does not affect the ability of organisations to store or link health their information electronically.

HPP 15 is designed to deal with electronic health records systems that link health records at a state or national level, for example:

- The Health e-Link electronic health records scheme in NSW
- The Health *Connect* electronic health records scheme at a federal level

It requires that such schemes must be “opt-in”, meaning that a patient must give express consent to participate.

PART 3: COMPLAINTS UNDER THE HRIP ACT

3.1 THE COMPLAINTS-HANDLING PROCESS

If a person believes that you have breached their health privacy, they can make a complaint about it under the HRIP Act. The complaints-handling processes for the public and private sectors are slightly different.

- *Complaints about the public sector*

For public sector organisations, the complaints procedure under the HRIP Act uses the complaints procedure under Part 5 the PPIP Act. That is, where a person believes your organisation has handled their health information in breach of the HPPs, the person can seek an internal review by your organisation. If the internal review is not completed within 60 days, or the person is unhappy with the handling or results of the internal review, they can ask the Administrative Decisions Tribunal to review the conduct or decision. The Tribunal can make legally binding orders, including ordering your organisation to correct its conduct or pay compensation of up to $40,000.

- *Complaints about the private sector*

Where a person believes your organisation has handled their health information in breach of the HPPs or the special private sector provisions in Part 4 of the HRIP Act, the person can make a complaint to the NSW Privacy Commissioner. When a complaint is received, if it is identified as being within the Commissioner's jurisdiction to investigate, your organisation will be notified as soon as possible and given details of the complaint.

The Commissioner may attempt to resolve the complaint by conciliation, or may further investigate the complaint and make a written report containing findings and/or recommendations. The Commissioner's findings and recommendations are not binding.

If the person is not satisfied with the Commissioner's findings, they can ask the Administrative Decisions Tribunal to review the conduct or decision. The Tribunal can make legally binding orders including ordering your organisation to correct your conduct or pay compensation of up to $40,000[1].

Footnotes - Part 1

[1] Personal information is defined in section 5 of the HRIP Act.
[2] 'Health service' is defined in section 4 of the HRIP Act.
[3] Section 5(1) of the HRIP Act.
[4] Section 5(1) of the HRIP Act.
[5] In the case of *Vice Chancellor, Macquarie University v FM*
[2003] NSWADTAP 43 (determined under the PPIP Act) two Macquarie University staff disclosed information about FM's conduct as a student of Macquarie University to the University of New South Wales. The information was disclosed during telephone conversations. There was no evidence that the information was previously written down or recorded in a material form by any staff member of Macquarie.

Macquarie argued that the meaning of personal information in s.4 of the PPIP Act is limited to information held in a material documentary form, for example, in paper records or electronic storage. Since the information disclosed to the University of New South Wales was merely held in the minds of the Macquarie staff members, Macquarie argued that such information was not protected by the Act. The Appeal Panel did not accept that the meaning of "information" could be read down in this manner.

Macquarie also argued that the PPIP Act does not protect information in the nature of perceptions and knowledge that is obtained independently of university record keeping or collection of data by the University. The Appeal Panel did not accept that the meaning of "personal information" could be read down in this manner.
[6] Including the special private sector provisions in Part 4 of the HRIP Act on access (Part 4, Division 3)
[7] Including the special private sector provisions in Part 4 of the HRIP Act on amendment (Part 4, Division 4)
[8] Refer to section 19(3) of the HRIP Act to see the list.
[9] Section 5(3)(a) of the HRIP Act
[10] Section 5(3)(m) of the HRIP Act
[11] Section 5(3)(n)
[12] De-identified information is information from which identifiers have been permanently removed, or where identifiers have never been included. De-identified information cannot be re-identified.
[13] The term 'public sector agency' is defined in section 4 of the HRIP Act.
[14] The term 'private sector person' is defined in section 4 of the HRIP Act.
[15] Section 9 of the HRIP Act sets out what constitutes 'holding' information.
[16] The exemption for small business operators is taken from the Federal *Privacy Act 1988.*
If you need more information on this exemption you should refer to section 6D of the Federal *Privacy Act 1988* and the definitions of that Act generally.
[17] Most of the HPPs contain a 'required or authorised by law' exemption. See for example **HPP 4(4)(c), HPP 5(2), HPP 6(2), HPP 7(2), HPP 8(4), HPP 10(2), HPP 11(2), and HPP 15(2).**
[18] These five elements of valid consent are reproduced from the Privacy NSW *Best practice guide on privacy and people with decision-making disabilities*
[19] Section 7 of the HRIP Act
[20] Section 8 of the HRIP Act

Footnotes - Part 2

[1] Section 10 of the HRIP Act.
[2] See the case of *Vice Chancellor, Macquarie University v FM* [2003] NSWADTAP 43, discussed above at footnote 5, Part 1, of this handbook.
[3] The case of *KJ v Wentworth Area Health Service* [2004] NSWADT 84 also involves the issue of sharing of health information among clinicians in a multidisciplinary treating 'team'. Here, KJ was receiving treatment for cancer in hospital. The notes of KJ's consultations with the hospital's psychologist and psychiatrist were placed on KJ 's general medical file held by the hospital. Please refer to the Privacy NSW website: **www.lawlink.nsw.gov.au/privacynsw** for the case notes.
[4] The term 'investigative agency' is defined in section 4 of the HRIP Act.
[5] Note that section 316 of the Crimes Act 1900 (NSW) also prohibits a person from concealing a serious indictable offence.
[6] HPP 10(5), and HPP 11(6)
[7] See section 75 and Schedule 2 of the HRIP Act.
[8] Section 4 of the HRIP Act.
[9] For health service providers in the public sector, the access fees and charges set out in DOH Circular 2002/22 will apply.

Footnotes - Part 3

[1] With the exception that if you are a non-corporate entity (for example an individual practitioner), the compensation is limited to $10,000.

This draft Handbook will be distributed for use for a four-month consultation period from September 2004 until December 2004 to assess its practical application. It is anticipated that a consolidated edition of the *Handbook to health privacy,* incorporating any changes arising from its first four months in operation, will be released by January 2005.

Your feedback is welcome on the contents of the Handbook.
Any comments should be directed to the address below:

Privacy NSW

Office of the NSW Privacy Commissioner
PO Box A123
Sydney South NSW 1235

web site: www.lawlink.nsw.gov.au/privacynsw
email: privacy_nsw@agd.nsw.gov.au

Phone: (02) 9268 5588
Fax: (02) 9268 5501
TTY: (02) 9268 5522

Reference: HRIPA01-2004-08