

## How to prepare for the NSW *Health Records and Information Privacy Act 2002*

### Introduction

The *Health Records and Information Privacy Act 2002* (the HRIP Act) creates a legal framework to protect the privacy of peoples' health information in NSW. It covers all public and private sector organisations in NSW that provide a health service or that collect, hold or use health information.

The HRIP Act commences on 1 July 2004.

Most organisations already have experience with privacy. NSW public sector agencies have been covered by the NSW *Privacy and Personal Information Protection Act 1998* (the PPIP Act) since 1 July 2000. Most NSW private sector organisations have been covered by the Commonwealth *Privacy Act 1988* since 21 December 2001. You will find that if your organisation is already complying with existing privacy laws, the HRIP Act should not impose any significant additional obligations.

However the HRIP Act does provide more detailed rules on the way your organisation must handle health information. The impact of the HRIP Act on some organisations will be greater than on others. Preparing for the HRIP Act is something that has to be done *by* organisations. It cannot be done *to* them or *for* them. This publication explains seven steps that your organisation can go through to help prepare for the HRIP Act.



#### Tip for public sector organisations:

Up until now, the PPIP Act has protected the privacy of all personal information (including health information) collected or held by NSW public sector agencies. With the commencement of the HRIP Act, 'health information' will be taken out of the PPIP Act. So, as at 1 July, the PPIP Act will no longer regulate health information, but will continue to regulate all other personal information collected or held by NSW public sector agencies. Health information will be specifically protected by the HRIP Act.



#### Tip for private sector organisations:

If your organisation has privacy obligations under both the Commonwealth *Privacy Act 1988* and the HRIP Act, you should comply with both Acts concurrently. This should be possible in most cases, however the Australian Constitution says that when a law of the State is inconsistent with a law of the Commonwealth, the latter will prevail to the extent of the inconsistency.

## Step 1: Familiarise yourself with the meaning of 'health information'

As the HRIP Act protects 'health information', you and other members of your organisation should be familiar with what 'health information' is. 'Health information' is a specific type of personal information. It is defined in section 6 of the HRIP Act. It includes personal information that is information or an opinion about:

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

If your organisation is a health service provider, 'health information' includes all of the above plus:

- ◆ any other personal information collected to provide, or in providing a health service.

'Health service' and 'health service provider' are defined in section 4 of the HRIP Act.

## Step 2: Identify where and how your organisation handles health information

Step 2 is to identify where and how your organisation handles health information. If your organisation is a health service provider, most of the information it handles will be classified as health information. However you should not make assumptions here. Even if your organisation is not a health service provider, chances are it will still handle health information. Local councils, for example, may handle health information in the course of providing family day care, community care, or aged and disability support services.

You should involve as many members of the organisation as possible in the identification process. Although most organisations will already have a privacy contact officer, in medium sized or larger organisations a single officer cannot reasonably be expected to know the course that health information takes through the organisation's structures. It may be useful to establish a privacy committee to oversee the identification process, if you do not already have one. The privacy committee could consist of representatives from all relevant parts of the organisation.

Questions your organisation should ask in the course of the identification process include:

### Collection

- ◆ What health information does the organisation collect?
- ◆ How does the organisation collect the health information?
- ◆ Why does the organisation collect the health information? Does the health information need to be collected to fulfil the organisation's functions?
- ◆ Are people notified of the collection, the purpose(s) for it, and any intended uses or disclosures of the health information?

### Storage

- ◆ Where and how does the organisation store the health information?
- ◆ Who has access to the health information held by the organisation? Who actually needs to have access?

- ◆ What measures does the organisation have to protect health information from unauthorised access, modification, misuse, loss or disclosure? Do they need to be improved?

### **Access and accuracy**

- ◆ Is the organisation able to easily provide people with access to their own health information?
- ◆ Is the health information accurate, complete and up-to-date?

### **Use**

- ◆ How does the organisation use the health information?

### **Disclosure**

- ◆ Does the organisation disclose the information to anyone outside the organisation?
- ◆ Does the organisation transfer health information interstate or overseas?

You may also use the identification process as an opportunity to examine the flow of other types of personal information within your organisation.

## **Step 3: Familiarise yourself with the 15 health privacy principles (HPPs)**

As part of the identification process, members of your organisation should familiarise themselves with the 15 health privacy principles (HPPs). The HPPs are the key to the HRIP Act. They are legally binding rules set out in Schedule 1 of the HRIP Act. They regulate the way an organisation can collect, store, use or disclose health information. You will find a plain English summary of the HPPs in Privacy NSW Fact Sheet #4 and at the end of this publication.

## **Step 4: Review existing practices and make changes where necessary**

Run through each of the HPPs and think about how your organisation's health information handling practices measure up against them. Doing this will help your organisation to identify which practices comply and which may need to be changed in light of new legal requirements in the HRIP Act.

HPP 4 in particular sets out a requirement to notify people of certain things when you are collecting their health information. You may already have forms and publications which include details about the collection of your clients' and employees' personal information under the PPIP Act or the Privacy Act. You should review those forms and publications to see whether they need updating to also reflect the collection of health information.

## **Step 5: Approach implementation in an integrated way**

If your organisation is already covered by a privacy law, it is best to approach implementation of the HRIP Act in an integrated way. That is, you should integrate compliance with the HRIP Act into processes which are already in place to deal with existing privacy laws.

For example, your organisation's privacy policy statement could address the way that your organisation deals with personal information and health information under the privacy laws by which it is bound.



The preamble might state:

“This privacy policy details how the organisation deals with personal information and health information it collects to ensure that it complies with the *Privacy and Personal Information Protection Act 1998 (NSW)* OR *the Privacy Act 1988 (Cth)* and the *Health Records and Information Privacy Act 2002*. In the privacy policy, a reference to ‘information’ is a reference to both personal information and health information.”

A similar privacy regime exists in Victoria. You could look to some Victorian organisations for ideas about how to approach implementation in an integrated way. However ultimately implementing information privacy protection is unique to each organisation, and connected to the actual personal information that each organisation handles in its particular role. It is something that each organisation will have to undertake for itself.



#### **Tip for public sector organisations:**

NSW public sector organisations are also required to incorporate consideration of the HRIP Act into their existing Privacy Management Plan.

## **Step 6: Make sure your complaints-handling process deals with health information**

Your organisation should be ready to deal with health privacy complaints from 1 July 2004. Complaints may be made to you in the first instance, or they may be made direct to Privacy NSW. You may need to revise your existing complaints-handling process to ensure that your organisation can handle health privacy complaints effectively.



#### **Tip for public sector organisations:**

For public sector organisations, the complaints procedure under the HRIP Act mirrors the complaints procedure under the PPIP Act. That is, where a person believes your organisation has handled their health information in breach of the HPPs or in breach of a relevant Health Privacy Code of Practice, 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, the individual can ask the Administrative Decisions Tribunal to review the conduct or decision. The Tribunal can make legally binding orders.

As long as you already have systems in place to process applications for internal review under the PPIP Act, then you will only need to adapt those systems to incorporate complaints under the HRIP Act.

Generally speaking, complaints made direct to Privacy NSW about an alleged breach of the HPPs or relevant Health Privacy Code of Practice will be referred to internal review. However in some circumstances Privacy NSW will investigate a complaint rather than insist it be dealt with as an internal review. The Privacy Commissioner also has a general power under the PPIP Act to investigate complaints about the alleged violation of, or interference with, the ‘privacy’ of a person. ‘Privacy’ is not limited to ‘information privacy’ and may include breaches of ‘physical privacy’ (for example surveillance, bag checks) as well as complaints not strictly covered by the HRIP Act. An example is if a public sector organisation refused to conduct an internal review under the HRIP Act because the request



was made one day out of time. If there were good reasons, the Privacy Commissioner might still investigate that complaint under the general complaint-handling powers in the PPIP Act.



### **Tip for private sector organisations:**

Where a person believes that your organisation has handled their health information in breach of the HPPs, Part 4 of the HRIP Act, or a relevant Health Privacy Code of Practice, 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 practicable and given details of the complaint. Systems are needed to ensure correspondence from the Commissioner is responded to in a timely manner.

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. However if the person is still not satisfied, they can ask the Administrative Decisions Tribunal to review the conduct or decision at issue. The Tribunal can make legally binding orders.

Obviously it is better if your organisation can resolve complaints internally and directly without the intervention of Privacy NSW. This can save time and money, and give your organisation a chance to identify any systemic issues. It can also help restore the person's confidence in your organisation. Your organisation may be able to use existing complaints-handling procedures for any health privacy complaints. Alternatively your organisation may need to develop new procedures with the new health privacy requirements in mind.

Remember that the Privacy Commissioner also has a general power under the PPIP Act to investigate complaints about the alleged violation of, or interference with, the 'privacy' of a person. 'Privacy' is not limited to 'information privacy' and may include breaches of 'physical privacy' (for example surveillance, bag checks) as well complaints not strictly covered by the HRIP Act.

## **Step 7: Train staff and promote awareness**

Your organisation's ability to comply with the HRIP Act is very much dependent on its staff members and how they handle health information. As those of you subject to existing privacy laws will be aware, the more people in the organisation who know about the HRIP Act, the more likely it is that your organisation will be operating in compliance with the HRIP Act.

Staff members should be made aware of the HRIP Act, in terms of their responsibilities and their own rights. For example you could use any internal communication mechanisms within your organisation – for example staff newsletters, emails, or notice boards - to circulate information about the HRIP Act.

Staff members should also be encouraged to train on the HRIP Act.

NSW Health is offering training to organisations in the NSW public health system. For more information please contact NSW Health on (02) 9391 9092.

Privacy NSW is offering training to all other organisations covered by the HRIP Act. For more information please contact Privacy NSW on (02) 9928 5588.



## To find out more

### How to obtain a copy of the HRIP Act

To consult the HRIP Act online follow the links on the Privacy NSW website (see below).

To order a paper copy of the HRIP Act, call the NSW Government Bookshop on (02) 9238 0950 or fax (02) 9228 7227. The cost is \$11.00 over the counter or \$17.50 by post.

### How to contact Privacy NSW

Privacy NSW  
Office of the NSW Privacy Commissioner

web site: [www.lawlink.nsw.gov.au/privacynsw](http://www.lawlink.nsw.gov.au/privacynsw)

email: [privacy\\_nsw@agd.nsw.gov.au](mailto:privacy_nsw@agd.nsw.gov.au)

phone: (02) 9268 5588

fax: (02) 9268 5501

mail: PO Box A123  
Sydney South NSW 1235

office: Level 17, 201 Elizabeth Street  
Sydney NSW 2000

# 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 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.

*The material in this publication is intended only to inform. It has been simplified and should not be relied on as legal advice. The summary of the HPPs is a guide only and not a full statement of your obligations. You should consult the full text of the HPPs as well as Part 3 of the HRIP Act (public sector organisations) and Part 4 of the HRIP Act (private sector organisations) for a full statement of your obligations. If in doubt, please contact your Privacy Contact Officer or call Privacy NSW on (02) 9268 5588 or write to [privacy\\_nsw@agd.nsw.gov.au](mailto:privacy_nsw@agd.nsw.gov.au) for more information.*

*Privacy NSW accepts no liability for loss or damage that may be suffered by any person or entity that relies on information in this publication.*

*Copyright is owned or controlled by the Office of the NSW Privacy Commissioner unless otherwise indicated. Copyright in materials from third parties may be owned by others. Permission to reproduce their work should be separately sought.*

*Privacy NSW aims to make information about privacy readily available. The contents of this publication may be copied and used for educational and non-commercial use. The material should be used fairly and accurately and this publication and Privacy NSW should be acknowledged as the source. The authors of material, where known, should be credited, consistent with the moral rights provisions of copyright law.*

## **Privacy NSW**

Office of the NSW Privacy Commissioner

PO Box A123  
Sydney South NSW 1235

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

[www.lawlink.nsw.gov.au/privacynsw](http://www.lawlink.nsw.gov.au/privacynsw)

Reference: AS02-2004-02

© Privacy NSW 2004



privacynsw