information and privacy commission
new south wales

Advancing privacy in your agency

Participant manual

IPC Seminar

December 2012

Contents

What is the NSW privacy legislation?

- ***Privacy and Personal Information Protection Act 1998*** **(PPIP Act)**

  – The PPIP Act covers all of the NSW public sector agencies and provides reserve power for the Privacy Commissioner. The Act provides for the protection of personal information, and for the protection of the privacy of individuals generally

- ***Health Records and Information Privacy Act 2002*** **(HRIP Act)**

  – The HRIP Act covers all organisations in NSW that deal with health-related information and makes provision for the protection of health records and information.

Effective privacy protection depends on all staff of an agency being aware of their obligations to protect the privacy of clients, other employees and members of the public, who come into contact with the agency.

The privacy legislation is not intended to interfere with the efficient operation of the agency or to detract from its service to the public. It should not prevent the agency collecting, using and disclosing information for its lawful purposes.

It is important to ensure that staff members have sufficient understanding of their privacy obligations to feel confident in handling information so as to meet the requirements of their work, while at the same time complying with NSW privacy legislation.

The PPIP Act

The Privacy and Personal Information Protection Act 1998 (PPIP Act) is about 'personal information' and relates to information that is collected and held by a NSW public sector agency. Public sector agency includes NSW state government agencies, local councils, universities.

The PPIP Act:

- provides for the protection of personal information, and for the protection of the privacy of individuals generally
- provides for the appointment of a Privacy Commissioner
- is built around the 12 Information Protection Principles (IPPs).

What is personal information?

Personal information is any information or opinion about an identifiable person. This could include:

- written records about a person
- a photograph or image of a person
- fingerprints or DNA samples that identify a person
- information about a person that is not written down, but which is in the possession or control of the agency.

Under NSW privacy legislation, personal information can be summarised as:

- information or an opinion;
- is about an individual; and
- the individual's identity needs to be apparent or reasonably ascertainable.

Section 4 of the PPIP Act defines personal information as "information or an opinion… about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion".

Exemptions

The PPIP Act includes a number of exclusions to the definition of personal information – s4(3).

Personal information does not include information:

- about an individual who has been dead for more than 30 years
- in a publicly available publication
- about an individual's suitability for employment in the public sector
- which is contained in a public interest disclosure.

See Section 4(3) of the PPIP Act for a full list.

Under Section 4(4) of the PPIP Act, personal information is 'held' by an agency if:

- the agency is in possession or control of the information; or
- an employee of the agency is in possession or control of the information in the course of their employment or engagement; or
- the information is contained in a state record for which the agency is responsible.

Under the PPIP Act (Section 4(5)), personal information is not considered as collected by a public sector agency if the information is unsolicited.

The HRIP Act

The *Health Records and Information Privacy Act 2002* (HRIP Act) is about 'health information' and related to NSW government agencies and some private sector bodies such as health service providers as it covers all organisations in NSW that deal with health related information.

The HRIP Act:

- makes provision for the protection of health records and information (in both the public and private sectors)
- enables individuals to gain access to their health information
- provides an accessible framework for the resolution of complaints regarding the handling of health information
- is built around the 15 Health Privacy Principles (HPPs).

Both 'personal information' and 'health information' are defined in the HRIP Act. Under Section 5 of the HRIP Act, the definition of personal information is the same as under the PPIP Act. Many, but not all, of the exclusions are the same. See Section 5(3) of the HRIP Act and Section 4(3) of the PPIP Act for comparison.

What is health information?

Under Section 6(a) of the HRIP Act "health information" is defined as personal information about:

- An individual's physical or mental health, or disability;
- An individual's expressed wishes about the provision of health services;
- A health service provided to an individual;
- The term health information also includes other personal information collected to provide a health service (Section 6(b)).

The HRIP Act applies to 'health information' that is collected, held or used by a 'health service provider'. The definition of 'held' is consistent with the PPIP Act.

Health information is not considered 'collected' if the organisation does not ask for the information. Once the organisation records the information though, it is considered 'held'.

‘Health service’ is broadly defined in the HRIP Act and includes a list of services (including alternative services), whether provided as public or private services under definitions in Section 4. An agency or organisation does not need to provide a health service to collect or hold health information.

The HRIP Act also defines capacity (s7) and authorised representative (s8). The PPIP Act does not. The HRIP Act additionally defines child and parental responsibility (s8(3)).

In summary:

- The definition of personal information is not limited to what is considered private or the personal affairs of a person
- The definition of personal information is not limited to information contained in records. Personal information can include information or opinions that may not be recorded in written form
- There are exemptions to the definition of personal information. These exemptions are similar but not the same in the Privacy legislation
- Both the PPIP Act and HRIP Act use privacy principles that agencies must abide by in their conduct. Unless an exemption applies, agencies must comply with the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs).

Privacy Management Plans

Every NSW public sector agency that is bound by the PPIP Act must prepare and implement a privacy management plan that explains:

- The agency's policies and practices for complying with the PPIP Act and the HRIP Act
- How the agency will make its staff aware of these policies and practices
- The agency's procedures for dealing with privacy internal reviews under Part 5 of the PPIP Act
- Other relevant matters relating to the protection of the personal and health information that the agency holds (Section 33 of the PPIP Act).

The Information and Privacy Commission NSW (IPC) has developed a number of resources to assist agencies in developing, implementing and reviewing their privacy management plans including:

- "A guide to developing privacy management plans"
- "Privacy management plan assessment checklist"

Further practical considerations are included on pages 12-16 of this resource.

Privacy management plans should address why and how your agency collects, uses and discloses health information. What health information does your agency collect and hold? Why?

The Information Protection Principles (IPPs)

The 12 Information Protection Principles (IPPs) are the key to the *Privacy and Personal Information Act 1998* (PPIP Act). They are the legal obligations which NSW government agencies, for example government departments, local councils, universities, and local health districts must do when they collect, store, use or disclose personal information. Exemptions may apply.

The 12 IPPs are further detailed in the fact sheet "The Information Protection Principles (IPPs) – guidance for the public sector" which is available on our website under "Resources".

The 12 IPPs are found in Division 1 of Part 2 of the PPIP Act in sections 8 to 19. Each of these 12 sections addresses an information protection principle. Section 20 covers the general application of the IPPs to public sector agencies and section 21 provides for agencies to comply with the principles.

A useful way to look at the 12 IPPs is through the below five categories:

1. **Collection**
- Lawful, Relevant, Open, Secure

2. **Storage**
- Secure

3. **Access & Accuracy**
- Transparent, Accessible, Correct

4. **Use**
- Accurate, Limited

5. **Disclosure**
- Restricted, Safeguarded

The Health Privacy Principles (HPPs)

The 15 Health Privacy Principles are the legal obligations describing what NSW public sector agencies and private sector organisations, such as businesses, private hospitals, GPs, gyms etc, must do when they collect, hold, use or disclose a person's health information. Exemptions may apply. The HPPs are at Schedule 1, Sections 1 to 15. Each section addresses an HPP.

The 15 HPPs are further detailed in the fact sheet "The Health Privacy Principles (HPPs) – guidance for the public sector" which is available on our website under "Resources".

A useful way to look at the 15 HPPs is through the below seven categories:

1. **Collection**
   - Lawful, Relevant, Direct, Open

2. **Storage**
   - Secure

3. **Access & Accuracy**
   - Transparent, Accessible, Correct, Accurate

4. **Use**
   - Limited

5. **Disclosure**
   - Limited

6. **Identifiers & Anonymity**
   - Not identified, Anonymous

7. **Transferrals & Linkage**
   - Controlled, Authorised

At what point/s is your agency collecting personal information?

Working in small groups, identify the key questions you would need to ask within an agency about personal (and health) information under the category you have been allocated (it will be one of storage, access or disclosure).

Does your agency have any exemptions it should set out or are you exempted from complying with any IPPs/HPPs by your own legislation s25 PPIP Act/ s23 HRIP Act?

What Acts does your agency operate under/administer?

Practical guide for developing your privacy management plan

The following checklist is a list of considerations for agencies in developing their privacy management plan:

Who are you?

- Who is your organisation and how can it be contacted?
- What are your agency's main functions and the kinds of information it collects and holds to fulfill those functions?

How do you collect personal/health information?

- What personal/health information does your agency collect? Is this outlined clearly for clients, employees and members of the public?
    - Identify your agency's basic functions and activities to determine the type of information that is commonly collected to facilitate those functions.
        - Why is the information collected?
        - Is the collection directly from the individual concerned?
        - Is the collection reasonable?
        - Will the information be stored securely and for how long?
        - Does the agency outline how a person can ascertain if the agency has information in relation to them? (e.g. hold information on individuals)
        - Dos the agency set out how people can get access to information held by the agency?
        - Does the agency set out how a person can make arrangements to alter information it holds on individuals?
        - Does the agency check the accuracy of the information it holds?
        - Does the agency explain how it uses the information it collects?

How are the public made aware of your privacy policies and privacy management plan?

- How can client/employee/member of the public access their information held by your agency? Verbal/writing/email
- Is the collection of the information compulsory (at this point include any legislative requirements which authorise the collection, use or disclosure of the information, such as Local Government or Police (Law Enforcement) or it is optional. Does the collection help the client/employee/member of the public receive some kind of service or benefit?
- Does your agency have notification on forms of information it has collected advising what will happen with the information?

How do you use and disclosure information?

- How is the information used and to whom it is usually disclosed?
    - Does the agency explain why it would disclose information it holds?
    - Does the agency explain what information it cannot disclose, unless a serious or imminent threat to the life or health?

How are your staff made aware of the privacy management plan and their privacy responsibilities

- Does the plan make it obvious to staff what they can and can't do in relation to information they deal with within the workplace?
    - Consider why your agency is collecting the information.
    - Does the agency's information handling functions allow for a greater understanding of whether the agency is currently complying with the IPPs/HPPs in everyday work practice?
    - How do you deal differently if at all with sensitive information, e.g. do you give assurances to alleviate client fears, do you give information about access, and do you have an audit log in the likelihood of a complaint?
    - Is any of the information you collect required to be transferred out of the State of NSW?
    - How does any agency determine whether it complies with its own privacy management plan? A good way of assessing whether or not an agency is in compliance with its plan is with a self assessment using the IPC's assessment checklist.

- How is the plan available to clients/employees/members of staff?
    - i.e. internet, publication, downloadable, placing the privacy plan prominently at the front desk, in waiting room, meeting area.
    - Website, associated links.

How are internal reviews and complaints about breaches of privacy handled?

- Does the plan outline how to lodge an internal review under both s53 of the PPIP Act and s21 of the HRIP Act?
    - Does it inform the client/employee/member of the public of the agency's contact person if a complaint or request for an internal review is to be made?
    - Does it state the notification process of an internal review/complaint?
        - Notifying Privacy Commissioner of initial internal review
        - Notifying of progress (delays on track, draft findings)
        - Allow the Privacy Commissioner time to make submissions
        - Set out rights of review by the NSW Civil and Administrative Tribunal (NCAT) if dissatisfied with the outcome of the agency's internal review.
- Does the agency state if it has a complaint handling procedures in relation to privacy complaints, as opposed to a person making an internal review application?
    - Do you have a general customer service complaint handling function?
    - What is your procedure of reply? Email/post
    - Do you set out for the complainant we are dealing with this as a complaint, but if you are dissatisfied then you can lodge and internal review.
    - It is best to set out the options of (complaint/internal review) for the complainant and allow them to decide?

- When you receive a complaint via email, what is your process for response? Is that set out for the complainant, eg, if they email a query; is your policy to respond only to postal addresses? If so how do you match the name to the address through your internal systems?

Other considerations for inclusion in a privacy management plan

- Does the agency's plan state whether another law impacts on its privacy obligations in relation to the agency's core functions, i.e. do they operate under an exemption by way of s41 or s62 direction or a code of practice (if yes, make note of the exemption and how it alters what they can and can't do in relation to Acts)? Some exemptions may only apply at the time of the disclosure/research and not be applicable after the fact.

- Does the Agency's plan state whether they have public register/registers? Does it state how a person can make an application for access to the register/registers? Does the agency outline the options for suppressing public register information?

- Does the agency outline how it will maintain the training of staff to be aware of their privacy obligations in relation to their duties? i.e. training, providing brochures, induction material?

When should an agency review its privacy plan?

- Do you acknowledge that you may amend your plan at any time?
- An organisation should review its privacy plan from time to time, particularly as its understanding of privacy in its internal processes grows.
- If an agency begins to collect more information or uses or discloses information differently, this should be immediately reflected in the agency's privacy plan. Where an agency attains new functions or has undergone restructure, a review of its plan is necessary.

What if my agency is very similar to other agencies?

An agency may have similar structure to other agencies, particularly where agencies have similar functions (e.g. local government agencies). While there will be common material, it is important to remember that privacy plans need to be adapted to individual agencies, because every agency collects

and handles information differently. It is risky to simply copy another agency's plan. A plan should reflect an agency's own practices.

One policy may be sufficient, depending on the size of the agency and its functions. Most NSW government agencies contain many different offices that have vastly varying functions to one another (for example, the Department of Justice or the Department of Human Services). In these cases, it may be advisable for each business unit to have its own plan. Other government agencies may need to have a number of polices to cover different types of information or information handling practices (for example, separate website and employee e-mail monitoring policies, and a privacy plan covering general functions).

Further resources

- For more detailed advice on developing your privacy management plan see the IPC's "A guide to developing privacy management plans"

- To review your agency's privacy management plan (either as a draft or part of your review cycle), see the IPC's "Privacy management plan assessment checklist"

Both resources are included in the kit for the "Advancing privacy in your agency" seminar.

What you need to do with your privacy management plan

- Provide a copy to the Privacy Commissioner as soon as possible (section 33(5) of PPIP Act). The Privacy Commissioner has a responsibility to provide assistance and feedback with plans. We do not however provide legal advice or endorse plans.

- Publish the plan on your website with your other open access information (as required under the *Government Information (Public Access) 2009* (GIPA Act).

- Circulate the plan to your staff and ensure they receive targeted privacy training for the privacy issues identified in your plan.

- Think about having copies of your plan available in your public spaces, such as at reception, in waiting or meeting rooms.

- Note in your next annual report that you have prepared/reviewed your privacy management plan.

- *Add your own ideas or those shared by other participants…*

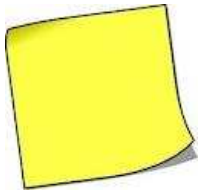
Once your privacy management plan is in place

Your ‘guide to making privacy management plans’ and the ‘assessment checklist’ will have many general tips for things to do once you have developed your privacy management plan. Some additional suggestions include:

- Use the self assessment checklist to identify any gaps/missing information
- Get someone with fresh eyes to look at your plan and give you feedback (e.g. a new staff member, a stakeholder)
- Set a review date and communicate this in your plan so you are committed to it
- Get sponsorship of the plan by your senior management and have privacy issues as a standard agenda item in your Executive meetings
- Refer your plan to your Risk and Audit committees for feedback and review
- *Add other your own ideas or those shared by other participants below*

How to use your privacy management plan to promote privacy

- Set the review date of your privacy management plan to be shortly before Privacy Awareness Week (PAW) so that privacy issues will have prominence in your agency. Privacy Awareness Week (early May each year) is an opportunity to encourage your agency's staff to address a particular Information Privacy Principle or a Health Privacy Principle.
- Record a brief message that telephone callers can opt to hear, detailing your agency's privacy compliance.
- Develop a layered privacy notice, if your agency doesn't yet have one. This offers a condensed snapshot of your agency's privacy management plan and helps people access and understand your privacy policy and practices.
- Prepare a log-in screen for all of your agency's computers that contains messages reminding staff of the importance of privacy.



During Privacy Awareness Week (PAW) specifically:

- Think about launching any significant new privacy initiatives or re-launch your revised privacy management plan

- If your privacy management plan has not been recently reviewed, encourage staff to revisit the plan and give you feedback (you could use a condensed version of the self assessment checklist to get their feedback)

- Send an email at the beginning of PAW to all staff explaining what the week is about and reminding staff of their privacy responsibilities. If possible, have your agency head send out this email as a way of showing your agency's overall commitment to good privacy practice.

- Display PAW posters and use other PAW resources to remind staff of their privacy obligation. Consider adding your agency's privacy contact officer's details to the posters to promote the role. Consider a display of posters and privacy materials on a table in your office's general staff area such as tea-room (not just your public places).

- Consider publishing an article about privacy on your agency's intranet. What are the privacy challenges that your agency and staff face? How does your agency effectively address privacy challenges? Or how could these challenges be met? Consider publishing an article about privacy in your agency's newsletter or on its website.

- Hold a training/information session on privacy. This could be a detailed training session that you schedule during PAW week, or just an information session outlining issues around collection or security of personal information.

- Look at and familiarise yourself with the PAW week resources available through the IPC's website or http://www.privacyawarenessweek.org/ directly. Each year there are specific themes and resources that agencies can use to promote privacy within their agency.

- Run a quick privacy quiz in your team. You could base it on, for example, the Health Privacy Principles or the Information Protection Principles. PAW usually have activities that you can use within your team e.g. survey's, quizzes, videos on specific privacy issues. PAW resources from previous years are archived on http://www.privacyawarenessweek.org/ and still available for use, or at least review, e.g. the 2011 campaign featured Zoggel through a short humorous animation showed the potential implications at work of your personal use of social media personally when your profile is not really private.

- Suggest all staff undertake the 'ID – theft tool', an easy self-assessment tool available at http://www.privacyawarenessweek.org/ as a PAW 2012 resource. Staff can test themselves on how aware they are about their risk of ID theft.