information and privacy commission new south wales

Guide to making privacy management plans

August 2012

Contents

A guide to making privacy management plans

What is a privacy management plan?

Every NSW public sector agency that is bound by the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**) must prepare and implement a privacy management plan (**plan**) that explains:

- the agency's policies and practices for complying with the PPIP Act and the *Health Records and Information Privacy Act 2002* (**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).

What is the purpose of a plan?

An agency's plan:

- ensures that the agency has identified how the requirements of the PPIP Act and the HRIP Act apply to the personal and health information that it manages
- explains the agency's functions and activities and the main types of personal or health information that the agency deals with to carry out those functions and activities
- explains the agency's strategies to comply with the PPIP Act and HRIP Act
- provides staff with the necessary knowledge and skills to manage personal and health information appropriately
- ensures that members of the public understand:
- how to make a complaint or request an internal review if they consider that their privacy may have been breached
- how to request access to their personal or health information or an amendment of that information to ensure that it is accurate
- encourages the agency to be transparent and accountable in how it manages personal and health information.

What must be included in a plan?

We recommend that an agency considers including information about the following issues in their plans to comply with section 33 of the PPIP Act.

1. Policies and practices to comply with the PPIP Act and the HRIP Act

Section 33(2)(a) of the PPIP Act states that a plan must include provisions relating to:

"the devising of policies and practices to ensure compliance by the agency with the requirements of this Act or the Health Records and Information Privacy Act 2002, if applicable."

An agency's policies and practices should deal with the key areas of compliance under the PPIP Act and the HRIP Act, which are discussed below.

1.1. Personal and health information

Personal information is defined in section 4 of the PPIP Act and is essentially any information or opinions about a person where that person's identity is apparent or can be reasonably ascertained. Personal information can include a person's name, address, information about a person's family life, information about a person's sexual preferences, financial information, photos, etc.

Health information is a more specific type of personal information and is defined in section 6 of the HRIP Act. Health information can include, among other things, information about a person's physical or mental health such as a psychological report, a blood test or an Xray, or even information about a person's medical appointment.

An agency's plan should explain:

- the main kinds of personal and health information that the agency deals with
- how this information is relevant to the agency's functions and activities.

1.2. Compliance with the Information Protection Principles and Health Privacy Principles

The Information Protection Principles (**IPPs**) in the PPIP Act and the Health Privacy Principles (**HPPs**) in the HRIP Act apply to NSW government agencies and regulate the collection, storage, use and disclosure of personal and health information. The principles also give members of the public a right to request access to their personal or health information or to ask for amendments to that information to ensure it is accurate.

An agency must comply with the HPPs even if the agency is not directly providing a health service. Most agencies will hold some health information, for example, in relation to employees and their sick leave or workers compensation matters.

An agency's plan should include the agency's strategies to comply with the IPPs and the HPPs. Those strategies should refer to the main types of personal and health information that the agency deals with to carry out its functions and activities.

Examples of an agency's compliance strategies could include the following:

- processes to ensure that paper or online forms used to collect personal or health information notify individuals about relevant matters such as why their information is being collected, how it will be used and who it will be disclosed to
- appropriate security measures to protect personal and health information, with different levels of security depending on the sensitivity of the information (eg an agency may have passwords to access certain files or databases or may physically secure sensitive files in a locked room or cabinet)

- processes to ensure that people can easily request access to, or amendment of, their personal or health information. The agency may have a dedicated person or persons to deal with these requests, its own application forms, guidance material on the agency's website, etc
- specific policies that inform the public about how it deals with personal or health information in certain circumstances. For example, an agency that carries out investigations may have a policy which explains what the agency will do with the information that the complainant provides for the investigation. The agency may have strategies in place to encourage complainants to read this policy such as including a copy of the policy in a prominent location on its website or sending complainants a copy of this policy when they make a complaint to the agency.

An agency's plan may deal with each IPP and HPP separately. However, in some cases it may be more appropriate to discuss several principles together, for example, the collection principles (IPPs 1 to 4 or HPPs 1 to 4) or the use and disclosure principles (IPPs 9 to 11 or HPPs 9 to 11). We recommend that agencies adopt the approach that best suits their needs and audience.

1.3. Relevant exemptions in the PPIP Act or the HRIP Act

There are exemptions to the IPPs in the PPIP Act that explain the circumstances in which an agency need not comply with an IPP (Part 2, Division 3 of the PPIP Act). Exemptions to the HPPs are often included in the principles themselves; however, there are also some exemptions in other provisions of the HRIP Act (for example, Part 2).

A plan does not necessarily have to refer to all of these exemptions. However, if an agency regularly relies on one or more of these exemptions, then it may be appropriate for the plan to discuss the effect of that exemption. For example, law enforcement or investigative agencies may wish to explain the relevant exemptions that apply when they are carrying out law enforcement or investigative functions.

1.4. Relevant public interest directions

Under section 41 of the PPIP Act and section 62 of the HRIP Act, the Privacy Commissioner may make a public interest direction with the approval of the relevant Minister. A public interest direction may exempt an agency from complying with one or more of the IPPs or HPPs where it is in the public interest for the agency not to comply in particular circumstances.

If an agency regularly relies on a particular public interest direction then it may be appropriate for the plan to explain the effect of this direction. For example, an agency may rely on a direction that has been created to deal with a particular project or function of that agency.

1.5. Relevant privacy codes of practice

Privacy codes of practice are sometimes made under Part 3, Division 1 of the PPIP Act or Part 5 of the HRIP Act. A code can modify the operation of an IPP, an HPP or a public register provision in Part 6 of the PPIP Act. Alternatively, it can specify how one of these provisions will operate in a particular circumstance.

If an agency regularly relies on a particular code, then it may be appropriate to describe the effect of that code in the plan.

1.6. Public registers

Part 6 of the PPIP Act requires agencies with responsibilities for public registers to:

- satisfy themselves that personal or health information disclosed from a register is used for a purpose relating to the purpose of the register or the Act under which the public register is kept (section 57 of the PPIP Act), and
- comply with requests to suppress personal or health information from the register, where the agency is satisfied that the safety and well-being of any person would be affected by not suppressing that information (section 58 of the PPIP Act).

We recommend that a plan include details of:

- the agency's public registers containing personal or health information
- how the registers are made available to the public
- how an agency satisfies itself that information that is proposed to be disclosed from a public register will be used for a purpose relating to the register's purpose or the Act setting up the register
- how a person can ask for their personal or health information to be suppressed from a public register
- how the agency will deal with that request, including the criteria or thresholds that the agency uses to determine the request.

1.7. Offences under the PPIP Act and the HRIP Act

Parts 8 of the PPIP Act and the HRIP Act contain offences for certain conduct of public sector officials and other persons. For example, there are offences relating to:

- corrupt disclosure and use of personal and health information by public sector officials
- inappropriately offering to supply personal or health information that has been disclosed unlawfully.

An agency's plan should refer to the offence provisions and explain its strategies to minimise the risk of its employees committing an offence. For example, some of these matters may be dealt with in the agency's code of conduct or through the agency's targeted privacy training.

2. Procedures for privacy internal reviews

Section 33(2)(c) of the PPIP Act states that a plan must include provisions relating to:

"the procedures that the agency proposes to provide in relation to internal reviews under Part 5."

If a person considers that an agency has breached an IPP, an HPP, a privacy code of practice or a public register provision in the PPIP Act, the person is entitled to an internal review of that conduct by the agency. If that person is dissatisfied with the way the agency deals with the internal review or the agency's findings, they can then ask the Administrative Decisions Tribunal to review the conduct.

A plan should explain that an agency is required to follow the requirements in Part 5 of the PPIP Act when carrying out an internal review. An agency will follow that process whether the conduct relates to an alleged breach of the PPIP Act or the HRIP Act. A plan should briefly describe the main steps in this process and should also note that the agency will refer to the Privacy Commissioner's guidance materials when carrying out an internal review. In particular, see “A guide for conducting internal reviews” and “Internal review checklist on our website.

A plan should explain an agency’s other procedures for internal reviews, including:

- providing a website link to the agency’s internal review application form and details of where to send the form. A template application form can be found on our website
- nominating an appropriate person within the agency to deal with internal reviews (usually the agency’s Privacy Contact Officer)
- recording requests for, and outcomes of, internal reviews for annual reporting purposes (clause 6 of the *Annual Reports (Departments) Regulation 2010* and clause 10 of the *Annual Reports (Statutory Bodies) Regulation 2010*).

Some individuals with privacy concerns may not want to go through the internal review process. For example, they may have a minor privacy concern that can be resolved quickly and easily. In these circumstances, an agency may deal with the complainant’s concerns through a more informal complaint handling procedure if the complainant is happy with that approach.

An agency’s plan should explain how it will deal with privacy complaints that are not dealt with through the internal review process. The plan may need to refer to the agency’s other policies, if appropriate, for example, the agency’s general complaint handling policies.

A plan should also note that an individual can make a complaint to the Privacy Commissioner about an alleged breach of their privacy.

3. Privacy training and education

Section 33(2)(b) of the PPIP Act states that a plan must include provisions relating to:

“the dissemination of those policies and practices to persons within the agency.”

A plan should explain how the agency will comply with this requirement. The agency may wish to consider the following strategies:

- ensuring that staff receive a copy of the agency’s plan when they start working at the agency and are promptly notified of updates to the plan, where relevant
- training staff in the agency’s plan to help them understand how to deal with personal and health information in the workplace (eg induction program, sessions provided by the Privacy Contact Officer, specialised training for specific roles)
- encouraging staff to refer to the plan and/or to liaise with the agency’s Privacy Contact Officer if they are unsure about a privacy issue
- ensuring that staff can easily access a copy of the plan, for example, by including a copy on the agency’s website, at the agency’s front desk or in meeting rooms
- promoting privacy compliance in the workplace, for example, putting up privacy-related posters or organising privacy awareness initiatives as part of the annual Privacy Awareness Week
- giving third party contractors a copy of the agency’s plan and training them in privacy where necessary

- ensuring that members of oversight boards and committees are given a copy of the agency's plan, made aware of the agency's privacy requirements and any relevant areas of risk.

4. Other relevant material to include

Section 33(2)(d) of the PPIP Act states that a plan must include provisions relating to:

"such other matters as are considered relevant by the agency in relation to privacy and the protection of personal information held by the agency."

An agency may wish to consider including the following information in its plan:

- reference to any other policies that assist the agency to comply with the PPIP Act and the HRIP Act or that are privacy-related (such as record keeping policies or polices relating to workplace surveillance)
- the contact details for the agency's Privacy Contact Officer, who would usually:
- be the agency's internal privacy expert
- deal with privacy-related enquiries, internal reviews and complaints
- assist the agency with advice or assistance in relation to any of the agency's functions or projects that have privacy implications
- the contact details of the Privacy Commissioner and the Administrative Decisions Tribunal
- website links to any relevant information referred to in the plan such as:
- the full text of the NSW privacy legislation
- relevant resources on the Privacy Commissioner's website
- the agency's public registers, if they are available online
- a list of the agencies that the plan covers if applicable (for example, if the plan has been prepared by a principal agency and is intended to cover smaller agencies within the principal agency)
- a table of contents, so that relevant information can be found quickly and easily
- an adoption and review date for the plan.

How detailed does the plan need to be?

A plan needs to contain enough information so that the agency's staff can understand how to deal with personal and health information appropriately and where to go to find out more information about this (eg referring to other relevant policies, speaking to the agency's Privacy Contact Officer about specific privacy concerns, etc).

The plan should also contain enough information so that members of the public can understand:

- the agency's functions and activities
- the main kinds of personal and health information that the agency deals with to carry out its functions and activities

- the strategies that the agency has adopted to comply with the NSW privacy legislation
- how a person can request access to, or amendment of, their personal or health information
- how a person can request a privacy internal review or make a complaint about a breach of privacy.

The plan should focus on the agency's functions and activities and the main kinds of personal and health information that the agency deals with to carry out those functions and activities. It does not need to explain every minor activity of the agency or every possible type of personal or health information that the agency deals with. The plan should refer to its other relevant policies and procedures where possible rather than explaining them in detail or reproducing them.

Can an agency use another agency's plan?

Sometimes an agency may want to:

- copy another agency's plan,
- write one plan to cover multiple agencies, or
- rely on another agency's plan.

A plan must accurately reflect the functions, activities and practices of the agency or agencies it covers. In some cases it may be possible to copy or use another agency's plan. In other cases the functions, activities and practices of an agency may be so different that it would be more logical to write a separate plan.

If an agency copies or uses another plan, it should tailor the plan to reflect its own functions, activities and practices.

If an agency intends to write one plan to cover multiple agencies, it must:

- list the agencies the plan covers
- ensure the plan accurately reflects the functions, activities and practices of each agency it covers
- ensure that each agency's website includes a link to that plan.

If an agency intends to rely on another agency's plan, it must:

- ensure the plan accurately reflects the functions, activities and practices of the agency
- contact the other agency to find out whether it intended the agency to be covered by that plan
- request the other agency to include its name on the list of agencies the plan covers
- include a link to the plan on its website.

What should an agency do once a plan has been prepared?

Before finalising the plan, the agency should seek approval and support from management using the agency's regular approval processes.

An agency must provide a copy of its plan to the Privacy Commissioner as soon as practicable after it has been finalised (section 33(5) of the PPIP Act). One of the functions of the Privacy Commissioner is to provide assistance to agencies in preparing and implementing plans. The Privacy Commissioner may provide assistance and feedback on plans. However, the Privacy Commissioner cannot provide legal advice or endorse plans.

An agency should also publish its plan on its website as open access information under the *Government Information (Public Access) Act 2009*. An agency may also wish to place its plan in a prominent place such as at its front desk, in a waiting room or in a meeting area to remind staff about the plan and to encourage members of the public to read the plan. An agency should also add references to the plan on forms that collect personal or health information.

An agency should circulate its plan to all staff and train staff in relation to the privacy issues identified in the plan, such as in an induction program. Staff should know to mention the plan to members of the public when collecting personal or health information and provide a copy if requested.

An agency can feature its plan and other privacy information for staff and members of the public as part of the annual Privacy Awareness Week.

An agency can use this plan to monitor privacy compliance and highlight relevant issues and complaints to its audit and risk committee and have a standing item on executive management meeting agendas.

When an agency prepares its next annual report, it should note that it has prepared a plan and explain any other action it has taken to comply with the NSW privacy legislation.

When should an agency review and update its plan?

The PPIP Act provides that an agency may amend its plan from time to time. The Privacy Commissioner encourages an agency to review its plan at regular intervals, such as every 12 months, or preferably no more than every two years. An agency should set a review date and communicate it clearly in the plan.

An agency should definitely review and update its plan when the agency's functions, structure or activities change or when technological advances or new systems change the way the agency manages personal or health information.

When amending a plan, an agency must send a copy of the amended plan to the Privacy Commissioner, preferably with the changes highlighted.

What issues could an agency consider before preparing a plan?

A plan should be written in plain English and be easy to read and understand. Agencies should ask themselves the following key questions to assist them to target their plan to their audience:

- What do members of the public need or want to know about how their personal and health information is managed by the agency?
- What do staff need to know to handle personal and health information appropriately?

The questions set out below are intended to assist agencies before they start preparing their plan. The list is not exhaustive and an agency may also want to consider other relevant questions. These questions are intended to help agencies in determining the kinds of information that they will need to gather before preparing their plan.

Agencies may also be interested in our "Privacy Management Plan Assessment Checklist". This checklist can be of assistance once an agency has prepared a plan and wants to confirm whether the plan covers all the key requirements.

Collection

- What types of personal and health information are collected by the agency (eg names, contact details, medical certificates, signatures, photographs/footage)?
- How is this information collected (eg over the phone, written correspondence, caller ID, recordings, CCTV footage)?
- What functions of the agency do these collections of personal and health information correspond with?
- Is the collection of personal or health information a legal requirement or is it voluntary?
- Is the collection of this information reasonable?
- Whose personal or health information is it (eg members of the public, employees, contractors, job applicants)?
- Does the agency collect personal or health information directly from the person whose information it is or from third parties?
- Does the agency's application forms contain appropriate notifications to make individuals aware of why their information is being collected, how it will be used and who it will be disclosed to?

Storage

- Where is this personal or health information stored (eg electronic or paper files)?
- How is the information kept secure and protected from unauthorised access?
- How long is the information stored for and is it destroyed securely once it is no longer required?
- Does the agency hold any particularly sensitive personal or health information? If so, is this information subject to stricter security controls?
- Does the agency use cloud storage, and if so, does it comply with IT security requirements?

Access and transparency

- Is the agency transparent in providing details on the personal or health information that it holds, why it holds that information, and how it can be accessed?
- Does the agency have procedures for dealing with applications for access to, or amendment of, personal or health information?

Use and disclosure

- What are the main purposes for which the agency uses and discloses personal or health information?

- Who within the agency can access personal and health information (eg HR section, enquiry staff, complaints and investigation officers, medical practitioners, contractors)?
    - Does the agency regularly disclose or transfer personal and health information to:
    - other sections within the agency, or
    - individuals or organisations outside the agency, or
    - Commonwealth agencies, or
    - individuals or organisations in other States or Territories within Australia or overseas?
- If the answer to the question above is yes, does the agency impose contractual or other conditions on the use or disclosure of personal or health information in any of those circumstances?
- In what circumstances does the agency seek consent first before using or disclosing personal or health information?
- Does the agency regularly disclose any sensitive personal information such as information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities?

Exemptions, codes of practice, other legislation and policies

- Does the agency regularly rely on any exemptions in the PPIP Act or the HRIP Act?
- Is the agency covered by any codes of practice or public interest directions under the PPIP Act or the HRIP Act?
- Are there any pieces of legislation applicable to the agency that authorise or require non-compliance with an IPP or an HPP?
- If the answer to any of the above is yes, how does this affect how personal and health information is collected and managed by the agency?
- Does the agency have any other policies relevant to the plan?

Public registers

- Does the agency have any public registers that contain personal and health information?
- How is this information disclosed?
- Does the agency have procedures in place to allow people to apply for their personal or health information to be suppressed from public registers?

Internal reviews and complaints processes

- How can a person seek an internal review?
- What is the internal review process?
- How does the agency appoint an appropriate person to deal with internal reviews?
- What is the role of the Privacy Commissioner in the internal review process?

- Where can a person go if dissatisfied with the agency's internal review?
- How does the agency report on internal reviews?
- Does the agency have an alternative complaint process if the person does not want to seek an internal review?

Public awareness and staff training

- How does the agency notify members of the public what personal and health information is being collected, what it is used for, who it is disclosed to, and how they can access it or amend it?
- How does the agency make staff aware of how to deal with personal and health information in compliance with the agency's policies and procedures and the NSW privacy legislation?

5. Document information

Title:	A guide to making privacy management plans
Business centre:	Information and Privacy Commission
Author:	Communications and Corporate Affairs
Approver:	Information Commissioner, CEO
Date of effect:	August 2012
Next review date:	December 2014
File reference:	
Keywords:	Privacy management plans, IPPs, public sector agencies, writing plans, compliance

6. Document history

Version	Date	Reason for amendment
1.1	July 2014	Document amended for accessibility