

A GUIDE TO
**MAKING
PRIVACY
MANAGEMENT PLANS**



Contents

1.	Background	1
2.	Purpose of Privacy Management Plans.....	2
3.	Requirements of a plan.....	3
3.1	Information Protection Principles and Health Information Principle.....	3
3.2	Privacy Codes of Practice.....	3
3.3	Internal Review	4
3.4	Public Registers	4
3.5	Training	5
3.6	Other Privacy Obligations	6
4.	Role of the NSW Privacy Commissioner	6
5.	Preparing a privacy management plan.....	7
	Privacy audit.....	7
	Current Protection.....	7
	Training	8
	Compliance	8
6.	Making the Plan	10
7.	Finalising the Plan.....	11
8.	Reviewing the Plan	11
9.	Further Advice	12

PRIVACY NEW SOUTH WALES

A Guide to Making Privacy Management Plans

This Guide includes the legislative minimum requirements for privacy management plans made under Part 3 Division 2 of the Privacy and Personal Information Act 1998 (the PPIP Act). It also makes suggestions about how to write a privacy management plan.

1. Background

Public sector agencies are required to prepare and implement privacy management plans (section 33 of the PPIP Act). This applies to all agencies meeting the PPIP Act's definition of a public sector agency (section 3).

A privacy management plan must cover (under section 33(2) of the PPIP Act):

- a) policies and practices to ensure compliance by the agency with the requirements of the PPIP Act and the Health Records and Information Privacy Act 2002 (the HRIP Act);
- b) how to disseminate these policies and practices to persons within the agency;
- c) procedures, which the agency proposes to follow, in relation to internal reviews under Part 5 of the PPIP Act and under the HRIP Act;
- d) other matters which the agency considers relevant to privacy and to the protection by the agency of personal and health information.

Compliance with the requirements of the PPIP Act includes compliance by an agency with the public register provisions in Part 6 of the PPIP Act.

We would also like to draw the attention of public sector employees to the parts of New South Wales privacy legislation, which relate to corrupt disclosure (Part 8 of the PPIP and HRIP Acts) and any other legislation relating to the disclosure of the information they hold.

A copy of an agency's privacy management plan must be provided to the New South Wales Privacy Commissioner as soon as practicable, after it has been prepared or amended (section 33(5) of the PPIP Act). Privacy management plans may be amended from time to time (section 33(4) of that Act).

2. Purpose of Privacy Management Plans

The purpose of a privacy management plan is to:

- ensure that the Agency has identified and considered the requirements of relevant privacy legislation (including principles, privacy exemptions and codes);
- identify collections of personal information and health information which are held by the agency or for which it is responsible;
- specify strategies which will ensure protective measures which are reasonably appropriate having regard to the kind of personal information and health information an agency collects and uses;
- develop a strategy for training staff to be aware of their obligations under privacy legislation and to be able to apply the principles flexibly and intelligently;
- ensure the appointment of a dedicated Privacy Contact Officer (PCO) to be a source of privacy expertise and help within an Agency.

The plan does not require the agency to demonstrate comprehensive compliance with privacy legislation, as long as it can show that the agency has identified privacy requirements and adopted strategies and policies for compliance. Privacy management is a continuous and evolving process reflecting the changing overall environment of information management. The plan, however, needs to be sufficiently detailed to allow agencies to use it in order to demonstrate a commitment to respecting the privacy rights of employees, clients, members of the public and others.

Privacy should not be equated with restrictions on the disclosure of information (confidentiality). Information privacy is designed to promote effective practices in the collection and use of personal and health information, which will assure clients, staff, members of the public and others that public sector agencies take a responsible and fair approach to their handling of information.

Personal and health information refer to reasonably identifiable information about individual humans and do not usually refer to aggregated and de-identified statistical information, information about corporations or organisations or about individuals, when they are acting in a public capacity.

Where, however, agencies incur obligations of confidentiality, which relate to personal and health information, either under specific legislation or the general law, the strategies for protecting this information should be included in the privacy management plan. The same is true of the agency's obligations under surveillance legislation e.g. the Surveillance Devices Act 2005 (NSW).

3. Requirements of a plan

Privacy management plans will need to address the following areas of compliance.

3.1. Information Protection Principles and Health Information Principles

The Information Protection Principles (IPPs) contained in the PPIP Act set out standards, which public sector agencies must follow, in relation to the way they process personal information.

Part 2 Division 2 of the PPIP Act specifies a number of exemptions from particular principles. Some of these apply to specific agencies, eg. law enforcement or investigative agencies. Others apply to specific kinds of proposed uses, for example, disclosure of information for revenue protection, investigative or law enforcement purposes.

For more detailed treatment of the privacy principles see Privacy New South Wales' pamphlet, "Your Privacy. Protecting Privacy in NSW" available on our website or in hard copy.

The Health Privacy Principles (HPPs) appear in Schedule 1 of the HRIP Act. There are also exemptions and exceptions to these. The HPPs also apply to the NSW private sector.

3.2. Privacy Codes of Practice

A public sector agency may decide to request the Privacy Commissioner to participate in negotiations, which may lead ultimately to the issue of a privacy code of practice. A privacy code of practice can modify the obligations of public sector agencies expressed in the IPPs or HPPs and must be approved by the relevant minister.

A code identifies those aspects of an agency's processing of personal information, which depart from the IPPs or the HPPs. The privacy management plan is a description of how an agency conforms to the IPPs, the HPPs or a relevant code. It is primarily concerned with operative policies and procedures, which relate to information processing requirements specific to the agency, including the use of particular systems or equipment.

Although it is primarily directed to compliance with the PPIP Act, a privacy management plan does not need to be as strictly limited in its content as a code. The plan can incorporate references to existing policies and documents, for example the agency's information technology security policy, its policies on surveillance, client or employee confidentiality or other protocols.

3.3. Internal Review

Any person in New South Wales can apply to a public sector agency for review of conduct, which they believe, contravenes a privacy principle, a privacy code of practice or the PPIP Act provisions about personal information kept in a public register. Section 55 of the PPIP Act provides for a further review by the Administrative Decisions Tribunal, which has the power to make binding orders.

Privacy management plans must specify the procedures that an agency proposes to follow in relation to internal reviews. These procedures should cover:

- any form provided by the agency for the purpose of making an application for internal review. (Privacy NSW has an application form which can be used for this purpose. It is on our website at www.lawlink.nsw.gov.au/privacynsw);
- the processing of applications and the designation of appropriate independent persons (e.g. the PCO) to conduct an internal review;
- the procedures to be followed in the conduct of an internal review and the notification of the outcome of a review (see also section 53 of the Administrative Decisions Tribunal Act 1997 (NSW)); and
- the recording of requests for, and outcomes of, internal reviews. This is required for reporting purposes, see section 33(3)(b) of the PPIP Act.

Carrying out an internal review is not the same as handling a privacy complaint. An effective system of complaint handling in relation to information privacy issues is likely to limit the number of internal review applications. Accordingly, agencies are advised to include complaint handling strategies in their privacy management plan. If privacy complaints are handled speedily and effectively, they may not proceed to an Application for Internal Review.

For further guidance on internal reviews, see Privacy New South Wales' Checklist on Interview Reviews available on our website: www.lawlink.nsw.gov.au/privacynsw

3.4. Public Registers

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

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

3.5. Training and Education

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. Privacy protection 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. Training should 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.

3.6. Other Privacy Obligations

Privacy management plans can also address:

such other matters as are considered relevant by the agency in relation to privacy and the protection of personal and health information held by the agency (section 33 (2)(d) of the PPIP Act).

4. Role of the NSW Privacy Commissioner

Under section 36(2) of the PPIP Act and section 58 of the HRIP Act the functions of the NSW Privacy Commissioner include:

- promoting the adoption of, and monitoring compliance with the IPPs and the HPPs;
- preparing and publishing guidelines relating to the protection of personal and health information;
- assisting public sector agencies in adopting and complying with the IPPs, the HPPs and privacy codes of practice;
- receiving and investigating complaints about privacy-related matters;
- assisting public sector agencies in preparing privacy management plans.

When investigating complaints about infringements of privacy, the Commissioner may decline complaints, which would be more appropriately dealt with by internal review. The Privacy Commissioner is to be notified by an agency of any request for internal review and may make a submission to an agency in relation to the review.

5. Preparing a privacy management plan

This section offers guidance on the steps to follow when drawing up a privacy management plan.

Privacy audit

5.1. Review the agency's collections of personal and health information e.g.

- a) is personal and health information collected for the use of a specific cost centre or is it available to the agency as a whole?
- b) is personal and health information stored
 - i. on computer databases?
 - ii. in paper files?
- c) do any of the agency's holdings fit the PPIP Act's definition of public registers?
- d) does the agency routinely transfer or disclose personal and health information to other public sector agencies or other organisations and individuals?
- e) does the agency routinely receive personal and health information from other public sector agencies or organisations or from individuals other than those, whom the information is about?

(Note: Many of the provisions of the PPIP and HRIP Acts refer to the lawful purpose, for which personal and health information is collected or used. Agencies should use the privacy management plan to carefully define these purposes. In many cases, these will provide a straight-forward basis for establishing whether a particular use or disclosure of the information is legal).

Current Protection

5.2. Identify existing policies which deal with protection of, and access to, personal and health information:

- a) are there specific legislative provisions restricting or authorising disclosure of information?
- b) is information disclosed to the agency or cost centre in circumstances giving rise to
 - i. a legal obligation of confidentiality?

- ii. professional ethical duties of confidentiality?
- c) Does the agency follow Archives Office/State Records Office authorisations for routine disposal of data no longer being used?
- d) Does the agency impose contractual or other conditions on the disclosure of personal and health information to other agencies or its provision to service providers (i.e. contracting out or outsourcing)?
- e) If the agency keeps a public registers, are there:
 - i. conditions on the way access is provided?
 - ii. arrangements to suppress information on the grounds of safety or well-being?

Training

5.3. Review staff training and awareness of the IPPs and HPPs:

- a) Identify staff with special responsibilities for handling personal and health information, e.g. client contact officers, keepers of public registers, counsellors or similar professionals;
- b) Identify materials used in staff training, which cover privacy and confidentiality requirements.

Compliance

5.4. Review the processes, whereby information is collected, for compliance with the first four information protection principles and/or health privacy principles:

- a) Do application forms and similar documents carry sufficient notification of the purpose for which information is collected and used by the agency?
- b) Do applications to inspect public registers allow the agency to establish the purpose for which personal information is required?
- c) Do officers collect information over the phone?
- d) Does the agency use automated means of capturing identifiable information, e.g. caller ID, videotape, recorded conversations with clients?

5.5. Review storage and security arrangements:

- a) Are record systems adequately designed to comply with the requirements of the PPIP and HRIP Acts and any other relevant legislation?
- b) What security arrangements apply to
 - i. paper files?
 - ii. computer files?
- c) Are these adequate in terms of risk management principles?
(Note: risk management in relation to information resources generally involves:
 - i. assessing the value of information resources for the agency, its clients and third parties who have an interest in the information;
 - ii. assessing the risk of loss, misuse or unauthorised disclosure of the information;
 - iii. assessing the effect on the agency, clients or information subjects of such loss, misuse or unauthorised disclosure;
 - iv. assessing the cost to the agency of minimising such risks).

5.6. Review the way personal and health information is processed administratively by the agency:

- a) Does the agency use personal and health information to confer benefits or entitlements on individuals?
- b) Does the agency rule on the qualification of individuals to perform a function, (e.g. occupational licensing)?
- c) Is the exercise of the above functions subject to an existing right of review?
- d) Does the agency have procedures to enable clients and employees to access and correct personal and health information?

5.7. Review disclosures to other agencies:

- a) Have the individuals concerned been notified at the time of collection of routine transfers to the specified agency/agencies?
- b) Are procedures in place to approve transfers in emergency situations?
- c) Does the agency transfer personal or health information to public sector agencies in jurisdictions outside New South Wales?

6. Making the Plan

The agency should now have a checklist of matters to serve as a basis for identifying strategies for compliance and drawing up the privacy management plan. The plan should incorporate the following features:

- a) It should be separately documented as a plan in compliance with the PPIP Act.
- b) It should identify significant collections of personal and health information and the purpose for which the information is collected and held.
- c) It should identify all corporate policies required to ensure compliance with the PPIP and HRIP Acts.

(Note: It is not intended that the management plan should itself provide details of every means taken to protect privacy, provided it refers to policies or procedures which do. For example, there are security reasons for not giving details of all steps taken to protect the security of information, although each agency should have an information security policy, which is known by, and available to, all employees, who have responsibilities to implement it.)

- d) Procedures should be defined for handling applications for internal review, including notification of internal review applications to the New South Wales Privacy Commissioner.
- e) Privacy complaint handling procedures should be in place as an alternative to internal review, so that privacy related issues can be easily and speedily resolved.
- f) Procedures should be defined for ensuring compliance with the public register provisions and ensuring that the agency can comply with a request to suppress personal information from public access without compromising the integrity of the register.
- g) The management plan should be sufficiently flexible to adapt to changing organisational arrangements and technology.
- h) Responsibility should be assigned to a competent officer or officers e.g. a Privacy Contact Officer (PCO) who is located within a section of the agency, which is appropriate for overseeing the operation of the plan and monitoring and reporting on outcomes.
- i) A privacy training and educational strategy for staff and third party service providers is crucial to the effectiveness of a plan.
- j) Inadequacies of record systems (which prevent an agency from complying with the IPPs or HPPs on such matters as notification, verification of accuracy, or amendment of information) should be identified and strategies

should be devised for addressing them (eg, more comprehensive notification at the time information is collected, privacy codes of practice).

7. Finalising the Plan

There is no legal requirement for an agency to obtain approval for its privacy management plan but the following requirements do apply to privacy management plans:

- a) The agency must provide a copy of its plan, or any amendment of the plan, to the New South Wales Privacy Commissioner as soon as practicable, after it has been prepared or made (section 33 (5) of the PPIP Act).
- b) The plan will provide a resource to enable agencies to comply with the requirements of sections 10 and 13 of the PPIP Act and HPPs 4 to 6 in the HRIP Act. In other words, the plan will describe the agency's practices in relation to the collection, storage and use of personal and health information.
- c) The functions of the Privacy Commissioner include providing assistance to agencies in preparing and implementing privacy management plans. The Privacy Commissioner's office cannot, however, provide legal advice on legal issues that may arise in relation to the agencies' handling of personal and health information. It is suggested that the agency take their own legal advice on this subject. A list of privacy advisers can be found on the website of the Federal Privacy Commissioner at: www.privacy.gov.au/links/service/index.html. In addition the services of the administrative law section of the Crown Solicitor's office are available to most public-sector agencies
- d) The annual report of an agency must include a statement of the action taken by the agency in complying with the PPIP Act and statistical details of any internal reviews conducted by or on behalf of the agency (section 33 (3) of the PPIP Act).

8. Reviewing the Plan

A privacy management plan should be reviewed at regular intervals and, if necessary, up-dated to take into account the agency's changing responsibilities, activities and technological means of processing information.

In particular, privacy management plans prepared before 2004 should be updated to take into account the provisions of the HRIP Act.

9. Further Advice

The Privacy Commissioner is concerned to ensure that the procedures for making privacy management plans are effective. We welcome any comments on these guidelines and on the management plan requirements of the PPIP Act. For comments, please contact:

Privacy New South Wales Locked Bag 5111 Parramatta NSW 2150, phone (02) 8688 8585, fax (02) 8688 9660, e-mail privacy_nsw@agd.nsw.gov.au

A privacy management plan can help ensure compliance of an agency with privacy legislation. It can be a very useful tool in providing guidance to staff, who deal with members of the public. A privacy management plan can also be of use in planning the policies of an agency.

The Privacy Commissioner recommends against using a template as the basis for a privacy management plan. Rather he urges public-sector agencies to attempt to dovetail their privacy management plans to their specific needs and structures. To assist you with this process, Privacy New South Wales will place a list of consultants on its website and these consultants will be contactable via Privacy New South Wales.

May 2009