Privacy Management Plans

Checklist

June 2014

Section 33 of the *Privacy and Personal Information Protection Act 1998* (PIPP Act) requires agencies to have a privacy management plan (plan). A plan sets out an agency's commitment to respecting the privacy rights of clients, employees and members of the public. It should also explain an agency's practices and procedures in handling personal information under the PIPP Act and health information under the *Health Records and Information Privacy Act 2002* (HRIP Act).

This checklist does not prescribe the structure and format a plan should follow. Rather, it is a useful tool for an agency to assess the content of its plan once it has already been prepared. The NSW Privacy Commissioner also uses this checklist to assess the quality of agency plans it receives.

For practical information on how to write a plan, please refer to the Guide to Making Privacy Management Plans.

Review Questions

General

1. Does the plan mention the agency's requirement to have a plan?

Yes ☐
Part ☐
No ☐
Comments

2. Does the plan describe the main kinds of personal and health information managed by the agency?
Tip: think about this question in context of the functions and activities of the agency

Yes ☐
Part ☐
No ☐
Comments

Information Protection Principles (Part 1, Division 1 of the PPIP Act)

3. Does the plan explain how the personal information the agency collects is related to the agency's functions and activities (IPP 1)? e.g. enquiries, complaints handling, core business, human resources, recruitment

Yes ☐
Part ☐
No ☐
Comments

4. Does the plan indicate when the agency collects personal information from the person and when it is collected from third parties (IPP 2)?

Yes ☐
Part ☐

No ☐
Comments

5. Does the plan explain how and when a person is notified that his/her personal information is being collected (IPP 3)?

Yes ☐
Part ☐
No ☐
Comments

6. Does the plan explain how the agency ensures that the collection of personal information is relevant, not excessive and is not an unreasonable intrusion (IPP 4)?

Yes ☐
Part ☐
No ☐
Comments

7. Does the plan generally explain how the agency stores, protects and disposes of personal information (IPP 5)?

Yes ☐
Part ☐
No ☐
Comments

8. Does the plan explain how the agency helps a person find out:

- whether the agency holds their personal information
- the nature of the information
- the main purpose for which it is collected
- his/her right of access (IPP 6)?

Yes ☐
Part ☐
No ☐
Comments

9. Does the plan set out how a person can access his/her personal information (IPP 7)?

Yes ☐
Part ☐
No ☐
Comments

10. Does the plan set out how a person can amend his/her personal information (IPP 8)?

Yes ☐
Part ☐
No ☐
Comments

11. Does the plan explain how the agency checks the accuracy of personal information before using it (IPP 9)?

Yes ☐
Part ☐
No ☐
Comments

12. Does the plan mention how the agency limits its use of personal information (IPP 10)?

Yes ☐
Part ☐
No ☐
Comments

13. Does the plan mention how the agency limits disclosure of personal information (including other jurisdictions) (IPP 11)?

Yes ☐
Part ☐
No ☐
Comments

14. Does the plan explain how the agency deals with sensitive personal information (IPP 12)?

Yes ☐
Part ☐
No ☐
Comments

Health Privacy Principles (Schedule 1 to the HRIP Act)

15. Does the plan explain how the health information the agency collects is related to the agency's functions and activities (HPP 1)? e.g. enquiries, complaints handling, core business, human resources, recruitment

Yes ☐
Part ☐
No ☐
Comments

16. Does the plan explain how the agency ensures that the collection of personal information is relevant, not excessive and is not an unreasonable intrusion (HPP 2)?

Yes ☐
Part ☐
No ☐
Comments

17. Does the plan indicate when the agency collects health information from the person and when it is collected from third parties (HPP 3)?

Yes ☐
Part ☐
No ☐

Comments

18. Does the plan explain how and when a person is notified that his/her health information is being collected (HPP 4)?

Yes ☐
Part ☐
No ☐
Comments

19. Does the plan explain how the agency stores, protects and disposes of health information (HPP 5)?

Yes ☐
Part ☐
No ☐
Comments

20. Does the plan explain how the agency helps a person find out:

- whether the agency holds their health information
- the nature of the information
- the main purpose for which it is collected
- his/her right of access (HPP 6)?

Yes ☐
Part ☐
No ☐
Comments

21. Does the plan set out how a person can access his/her health information (HPP 7)?

Yes ☐
Part ☐
No ☐
Comments

22. Does the plan set out how a person can amend his/her health information (HPP 8)?

Yes ☐
Part ☐
No ☐
Comments

23. Does the plan mention how the agency checks the accuracy of personal information before using it (HPP 9)?

Yes ☐
Part ☐
No ☐
Comments

24. Does the plan mention how the agency limits its use of health information (HPP 10)?

Yes ☐
Part ☐
No ☐
Comments

25. Does the plan mention how the agency limits disclosure of health information (HPP 11)?

Yes ☐
Part ☐
No ☐
Comments

26. Does the plan mention whether the agency assigns identifiers to individuals (if applicable) (HPP 12)?

Yes ☐
Part ☐
No ☐
Comments

27. Does the plan mention whether it gives individuals the opportunity to remain anonymous (HPP 13)?

Yes ☐
Part ☐
No ☐
Comments

28. Does the plan mention whether the agency discloses health information to individuals or bodies outside of NSW (HPP 14)? e.g. Commonwealth, interstate, overseas

Yes ☐
Part ☐
No ☐
Comments

29. Does the plan mention whether the agency includes health information in a health records linkage system (if applicable) (HPP 15)?

Yes ☐
Part ☐
No ☐
Comments

30. Does the plan mention whether any exemptions in the PPIP Act or the HRIP Act are particularly relevant to the agency?

Yes ☐
Part ☐
No ☐
Comments

Exemptions

31. Does the plan mention whether there are any particular codes of practice or public interest directions relevant to the agency?

Yes ☐
Part ☐
No ☐
Comments

32. Does the plan mention whether there is any relevant legislation that allows the agency not to comply with any of the IPPs or HPPs?

Yes ☐
Part ☐
No ☐
Comments

33. Does the plan mention whether the agency has any Memorandums of Understanding or referral arrangements with other agencies?

Yes ☐
Part ☐
No ☐
Comments

34. If any of the above are applicable, does the plan briefly explain how they actually impact on the agency's handling of personal or health information?

Yes ☐
Part ☐
No ☐
Comments

Public Registers

35. Does the plan advise whether the agency has any public registers that contain personal or health information?

Yes ☐
Part ☐
No ☐
Comments

36. If so, does the plan explain whether the personal or health information in these public registers can be accessed, and how?

Yes ☐
Part ☐
No ☐
Comments

37. Does the plan explain how a person can apply for personal or health information to be suppressed in a public register?

Yes ☐
Part ☐
No ☐
Comments

Internal Reviews and complaints

38. Does the plan explain a person's right to seek an internal review?

39. Does the plan set out the internal review process? e.g. how to apply for one, relevant timeframes, who makes the decision, how decisions are made, how the applicant is advised of the decision

Tip: if an agency does not have its own form, it can use the generic form on our website.

Yes ☐
Part ☐
No ☐
Comments

40. Does the plan explain the notification process and the role of the Privacy Commissioner?

Yes ☐
Part ☐
No ☐
Comments

41. Does the plan explain a person's right to an external review from the Administrative Decisions Tribunal if dissatisfied with the internal review outcome?

Yes ☐
Part ☐
No ☐
Comments

42. Does the plan set out the agency's alternative complaint process at the agency if a person wants to resolve an issue informally

Yes ☐
Part ☐
No ☐
Comments

43. Does the plan include the option to make a complaint to the Privacy Commissioner?

Yes ☐
Part ☐
No ☐
Comments

Offences

44. Does the plan generally explain the offences in the PPIP Act and HRIP Act?

Yes ☐
Part ☐
No ☐
Comments

Raising awareness of/using the plan

45. Does the plan set out how the agency trains staff to use the plan and comply with their privacy obligations? eg induction, periodic training, day to day work, what staff should do if unsure about a privacy issue

Yes ☐
Part ☐
No ☐
Comments

46. Does the plan set out how the agency educates members of the public in the agency's privacy obligations and their privacy rights? eg published on the web, mentioned on forms that collect personal or health information

Yes ☐
Part ☐
No ☐
Comments

Other agencies

47. Does the plan cover more than one agency?

Yes ☐
Part ☐
No ☐
Comments

48. If so, are the agencies listed individually?

Yes ☐
Part ☐
No ☐
Comments

49. Does the plan go into enough detail about the functions and the personal and health information managed by each agency covered?

Yes ☐
Part ☐
No ☐
Comments

Privacy-related policies and procedures

50. Does the plan describe how the agency devises its policies and practices to comply with the PPIP Act and the HRIP Act?

Yes ☐
Part ☐
No ☐
Comments

51. Does the plan specify whether there are other policies and procedures relevant to the plan?

Yes ☐
Part ☐
No ☐
Comments

52. If so, does the plan mention how the agency makes these documents available to staff and members of the public?

Tip: website links can be useful here

Yes ☐
Part ☐
No ☐
Comments

Accuracy

53. Is there an adoption/version date on the plan?

Yes ☐
Part ☐
No ☐
Comments

54. Is there a review date on the plan?

Yes ☐
Part ☐
No ☐
Comments

55. Are any references to legislation in the plan current?

Yes ☐
Part ☐
No ☐
Comments

56. If applicable, do the website links in the plan work?

Yes ☐
Part ☐

No ☐
Comments

Readability

57. Is the structure of the plan logical?

Yes ☐
Part ☐
No ☐
Comments

58. Does the plan have a table of contents?

Yes ☐
Part ☐
No ☐
Comments

59. Is the level of detail and length of the plan appropriate?

Yes ☐
Part ☐
No ☐
Comments

60. Is the plan written in plain English?

Tip: show your draft plan to a new staff member or a member of the public and ask whether they can understand it.

Yes ☐
Part ☐
No ☐
Comments

61. Is the plan helpful to members of the public and staff?

Yes ☐
Part ☐
No ☐
Comments

Contact details

62. Does the plan include current contact details for the Privacy Contact Officer or relevant privacy section at the agency for privacy-related enquiries?

Yes ☐
Part ☐
No ☐
Comments

63. Does the plan include current contact details for the Office of the Privacy Commissioner?

Yes ☐
Part ☐
No ☐
Comments

64. Does the plan include current contact details for the Administrative Decisions Tribunal?

Yes ☐
Part ☐
No ☐
Comments

Accessibility

65. Does the plan explain how the agency makes it available to staff and members of the public (eg website, over the counter, mailed out on request)?

Yes ☐
Part ☐
No ☐
Comments

66. Will the plan be on the agency's website and easy to find? Note: the plan is a policy document (open access information) under the Government Information (Public Access) Act 2009

Yes ☐
Part ☐
No ☐
Comments

General Comments

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Website: www.ipc.nsw.gov.au