Checklist

May 2026

Privacy Management Plans

Who is this information for?

NSW public sector agency staff seeking support on Privacy Management Plans.

Why is this information important?

This checklist can be used by public sector staff to assess the content of their agency's Privacy Management Plan once it has already been prepared.

Section 33 of the *Privacy and Personal Information Protection Act 1998* (**PPIP 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 PPIP 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 plans they receive from agencies.

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

Review Questions

	Yes	Part	No	Comments
General				
1. Does the plan mention the agency's requirement to have a plan?	☐	☐	☐	
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*	☐	☐	☐	
Information Protection Principles (sections 8 -19, 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*	☐	☐	☐	
4. Does the plan indicate when the agency collects personal information from the person and when it is collected from third parties (**IPP 2**)?	☐	☐	☐	
5. Does the plan explain how and when a person is notified that their 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**)?	☐	☐	☐	
7. Does the plan generally explain how the agency stores, protects and disposes of personal information (**IPP 5**)?	☐	☐	☐	
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 • their right of access (**IPP 6**)?	☐	☐	☐	
9. Does the plan set out how a person can access their personal information (**IPP 7**)?	☐	☐	☐	
10. Does the plan set out how a person can request an amendment to their personal information (**IPP 8**)?	☐	☐	☐	
11. Does the plan explain how the agency checks the accuracy of personal information before using it (**IPP 9**)?	☐	☐	☐	
12. Does the plan mention how the agency limits its use of personal information (**IPP 10**)?	☐	☐	☐	
13. Does the plan mention how the agency limits disclosure of personal information (including other jurisdictions) (**IPP 11**)?	☐	☐	☐	
14. Does the plan explain how the agency deals with sensitive personal information (**IPP 12**)?	☐	☐	☐	
Health Privacy Principles (clauses 1-15, 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*	☐	☐	☐	
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**)?	☐	☐	☐	
17. Does the plan indicate when the agency collects health information from the person and when it is collected from third parties (**HPP 3**)?	☐	☐	☐	
18. Does the plan explain how and when a person is notified that their 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**)?	☐	☐	☐	
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 • their right of access (**HPP 6**)?	☐	☐	☐	
21. Does the plan set out how a person can access their health information (**HPP 7**)?	☐	☐	☐	
22. Does the plan set out how a person can request an amendment to their health information (**HPP 8**)?	☐	☐	☐	
23. Does the plan mention how the agency checks the accuracy of health information before using it (**HPP 9**)?	☐	☐	☐	
24. Does the plan mention how the agency limits its use of health information (**HPP 10**)?	☐	☐	☐	
25. Does the plan mention how the agency limits disclosure of health information (**HPP 11**)?	☐	☐	☐	
26. Does the plan mention whether the agency assigns identifiers to individuals (if applicable) (**HPP 12**)?	☐	☐	☐	
27. Does the plan mention whether it gives individuals the opportunity to remain anonymous (**HPP 13**)?	☐	☐	☐	
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*	☐	☐	☐	
29. Does the plan mention whether the agency includes health information in a health records linkage system (if applicable) (**HPP 15**)?	☐	☐	☐	
30. Does the plan mention whether any exemptions in the PPIP Act or the HRIP Act are particularly relevant to the agency?	☐	☐	☐	
Exemptions				
31. Does the plan mention whether there are any codes of practice or public interest directions relevant to the agency?	☐	☐	☐	
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?	☐	☐	☐	
34. If any of 31 to 33 are applicable, does the plan briefly explain how they actually impact the agency's handling of personal or health information?	☐	☐	☐	
Public registers				
35. Does the plan advise whether the agency has any public registers that contain personal or health information?	☐	☐	☐	
36. If so, does the plan explain whether the personal or health information in these public registers can be accessed, and how?	☐	☐	☐	
37. Does the plan explain how a person can apply for personal or health information to be suppressed in a public register?	☐	☐	☐	
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.*	☐	☐	☐	
40. Does the plan explain the notification process and the role of the Privacy Commissioner?	☐	☐	☐	
41. Does the plan explain a person's right to an external review from the NSW Civil and Administrative Tribunal (**NCAT**) if dissatisfied with the internal review outcome?	☐	☐	☐	
42. Does the plan set out the agency's alternative complaint process at the agency if a person wants to resolve an issue informally?	☐	☐	☐	
43. Does the plan include the option to make a complaint to the Privacy Commissioner?	☐	☐	☐	
Mandatory Notification Data Breach (MNDB)				
44. Does the plan provide information on how data breaches will be managed by the agency?	☐	☐	☐	
45. Does the plan provide information on how to access the agency's Data Breach Policy and provide a link to the Policy?	☐	☐	☐	

	Yes	Part	No	Comments
46. Does the plan provide information on the process for assessing and notifying eligible data breaches to the Privacy Commissioner?	☐	☐	☐	
Offences				
47. Does the plan generally explain the offences in the PPIP Act and HRIP Act?	☐	☐	☐	
Raising awareness of the plan and using it				
48. Does the plan set out how the agency trains staff to use the plan and comply with their privacy obligations? *e.g. Induction, periodic training, day-to-day work, what staff should do if unsure about a privacy issue*	☐	☐	☐	
49. Does the plan set out how the agency educates members of the public in the agency's privacy obligations and their privacy rights? *e.g. Published on the web, mentioned on forms that collect personal or health information*	☐	☐	☐	
Other agencies				
50. Does the plan cover more than one agency?	☐	☐	☐	
51. If so, are the agencies listed individually?	☐	☐	☐	
52. Does the plan go into enough detail about the functions and the personal and health information managed by each agency covered?	☐	☐	☐	
Privacy-related policies and procedures				
53. Does the plan describe how the agency devises its policies and practices to comply with the PPIP Act and the HRIP Act?	☐	☐	☐	
54. Does the plan specify whether there are other policies and procedures relevant to the plan?	☐	☐	☐	
55. 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*	☐	☐	☐	
Accuracy				
56. Is there an adoption/version date on the plan?	☐	☐	☐	
57. Is there a review date on the plan?	☐	☐	☐	
58. Are any references to legislation in the plan current?	☐	☐	☐	
59. If applicable, do the website links in the plan work?	☐	☐	☐	

	Yes	Part	No	Comments
Readability				
60. Is the structure of the plan logical?	☐	☐	☐	
61. Does the plan have a table of contents?	☐	☐	☐	
62. Is the level of detail and length of the plan appropriate?	☐	☐	☐	
63. 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*	☐	☐	☐	
64. Is the plan helpful to members of the public and staff?	☐	☐	☐	
Contact details				
65. Does the plan include current contact details for the Privacy Contact Officer or relevant privacy section at the agency for privacy-related enquiries?	☐	☐	☐	
66. Does the plan include current contact details for the Information and Privacy Commission NSW (**IPC**)?	☐	☐	☐	
67. Does the plan include current contact details for the NSW Civil and Administrative Tribunal (**NCAT**)?	☐	☐	☐	
Accessibility				
68. Does the plan explain how the agency makes it available to staff and members of the public? *e.g. Website, over the counter, mailed out on request*	☐	☐	☐	
69. 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* (**GIPA Act)**	☐	☐	☐	
Automated Decision Making (ADM)				
70. Does the plan include a description of the types of ADM systems used, and their purpose? ***Note:** ADM refers to a fully or partially automated technical system, used in decision-making, which may or may not involve the use of AI, and affects people.*	☐	☐	☐	
71. Does the plan include information about the kinds of personal information used in ADM systems?	☐	☐	☐	

	Yes	Part	No	Comments
72. Does the plan describe the types of decisions made by ADM using personal information?	☐	☐	☐	
73. Does the plan explain who personal information may be shared with?	☐	☐	☐	
74. Does the plan describe the ways in which its use of ADM affects members of the public?	☐	☐	☐	
75. Does the plan include a process for how individuals can request more information?	☐	☐	☐	
76. Does the plan include information about how an individual can challenge or appeal a decision made by, or with the assistance of, ADM?	☐	☐	☐	
Artificial Intelligence (AI)				
77. Does the plan include a description of the types of AI systems used, and their purpose? ***Note:*** *AI refers to 'the ability of a computer system to perform tasks that would normally require human intelligence, such as learning, reasoning, and making decisions'. AI encompasses various specialised domains that focus on different tasks.*	☐	☐	☐	
78. Does the plan include information about the kinds of personal information used in AI systems?	☐	☐	☐	
79. Does the plan describe the way its use of personal information in AI affects members of the public?	☐	☐	☐	
80. Does the plan include a process for how individuals can request more information about the use of AI?	☐	☐	☐	
81. Does the plan include information about how an individual can challenge or appeal a decision made using AI?	☐	☐	☐	
82. Does the plan explain how and whether their personal information is used to train AI?	☐	☐	☐	
83. Does the plan explain how individuals may access their personal information held in AI systems?	☐	☐	☐	
84. Does the plan explain how information is shared with AI platforms and providers?	☐	☐	☐	
85. Does the plan explain where the information shared with AI platforms and providers is stored?	☐	☐	☐	

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

NOTE: The information in this checklist is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.