information and privacy commission new south wales

Fact Sheet **Updated November 2023**

Understanding your privacy obligations – for NSW public sector staff

Who is this information for?	NSW public sector staff
Why is this information important to them?	NSW privacy laws require NSW public sector agencies and staff to safeguard the privacy of the personal information they collect, store and use.

The *Privacy and Personal Information Protection Act 1998* (PPIP Act) outlines the basic obligations of NSW public sector agencies to protect the information that they collect about individuals. It also mandates what an agency must do when an eligible data breach occurs.

The *Health Records and Information Privacy Act 2002* (HRIP Act) deals with the handling of health information. The NSW Privacy Commissioner has the power to investigate privacy complaints under these laws.

Information Protection Principles (IPPs)

The 12 Information Protection Principles (IPPs) are your key to the PPIP Act. These are legal obligations which NSW government agencies, statutory bodies and local councils must abide by when they collect, store, use or disclose personal information.

What follows is summary of each of the principles, however, not all the exemptions have been listed. For a complete list of exemptions consult the legislation or, for further advice, contact the Privacy Contact Officer in your agency or the IPC.

Collection

1. Lawful (s. 8)

Only collect personal information for a lawful purpose[1] that is directly related to the agency's or organisation's activities and necessary for that purpose.

2. Direct (s. 9)

Only collect personal information directly from the person concerned, unless it is unreasonable or impractical to do so unless they have authorised collection of the information from someone else. Where the person is under the age of 16 years, the information about them may be collected from their parent or guardian.

3. Open (s. 10)

Inform the person as to why you are collecting their personal information, what you will do with it and who else might see it. Tell the person how they can view and correct their personal information and if there are any consequences if they decide not to provide their information to you.

4. Relevant (s. 11)

Ensure that the personal information collected is relevant, accurate, up-to-date, is not excessive and does not unreasonably intrude into the personal affairs of the individual.

Storage

5. Secure (s. 12)

Store personal information securely, keep it no longer than necessary and dispose of it appropriately. It should also be protected from unauthorised access, use or disclosure.

Access and accuracy

6. Transparent (s. 13)

Explain to the person what personal information about them is being stored, why it is being used and any rights they have to access it.

7. Accessible (s. 14)

Allow people to access their personal information without unreasonable delay or expense.

[1] A lawful purpose means a purpose that is not forbidden, rather than positively authorised, by law. *Norkin v University of New England* [2023] NSWCA 194

8. Correct (s. 15)

Allow people to update, correct or amend their personal information where necessary.

Use

9. Accurate (s. 16)

Make sure the personal information is relevant and accurate before using it.

10. Limited (s. 17)

Only use personal information if the person has given their consent to its use or they were informed of the use at the time of collection.

Only use personal information for the purpose for which it was collected, or a directly related purpose.

Personal information can be used without a person's consent in order to deal with a serious and imminent threat to any person's health or safety.

Disclosure

11. Restricted (s. 18)

Only disclose personal information with a person's consent or if the person was told at the time of its collection that it would be disclosed.

Personal information may be disclosed if the disclosure is for a purpose directly related to the original purpose of collection and the person is unlikely to object.

Personal information can be disclosed without a person's consent in order to deal with a serious and imminent threat to any person's health or safety.

12. Safeguarded (s. 19)

An agency cannot disclose sensitive personal information without a person's consent, including information about a person's ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. It can only disclose sensitive information without consent in order to deal with a serious and imminent threat to any person's health or safety.

An agency should not disclose personal information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless they are able to rely on one of the exceptions. For further information see the fact sheet here.

Health Privacy Principles (HPPs)

The 15 Heath Privacy Principles (HPPs) are located in Schedule 1 of the HRIP Act.

These are legal obligations which NSW public sector agencies and private sector organisations must abide by when they collect, hold, use and disclose a person's health information.

What follows is summary of each of the principles, however, not all the exemptions have been listed.

For a complete list of exemptions consult the legislation or, for further advice, contact the Privacy Contact Officer in your agency or the IPC.

Collection

1. Lawful

Only collect health information for a lawful purpose that is directly related to the agency's or organisation's activities and necessary for that purpose.

2. Relevant

Ensure health information is relevant, accurate, up-to-date and not excessive, and that the collection does not unreasonably intrude into the personal affairs of a person.

3. Direct

You should collect health information about a person directly from that person, unless it is unreasonable or impracticable to do so.

4. Open

Inform a person as to why you are collecting their health information, what you will do with it, and who else may see it. Tell the person how they can view and correct their health information and any consequences if they choose not to provide their information to you.

If you collect health information about a person from a third party you must still take reasonable steps to notify the person that this has occurred.

Storage

5. Secure

Ensure the health information is stored securely, not kept any longer than necessary, and disposed of appropriately.

Health information should be protected from unauthorised access, use or disclosure.

Access and accuracy

6. Transparent

Explain to the person what health information is being stored, the reasons it is being used and any rights they have to access it.

7. Accessible

Allow a person to access their health information without unreasonable delay or expense.

8. Correct

Allow a person to update, correct or amend their health information where necessary.

9. Accurate

Ensure that the health information is relevant and accurate before using it.

Use

10. Limited

Only use health information for the purpose for which it was collected or for a directly related purpose, which a person would expect. Generally, use for a secondary purpose would require the person's consent.

This principle is subject to a number of exceptions including use in cases of emergency, to lessen or prevent a serious threat to life, training, research and law enforcement purposes.

Disclosure

11. Limited

Only disclose health information for the purpose for which it was collected or for a directly related purpose that a person would expect. Other disclosures would generally require the person's consent.

This principle is also subject to a number of exceptions including use in cases of emergency, to lessen or prevent a serious threat to life, training, research and law enforcement purposes. There are also exceptions for disclosure for compassionate reasons and disclosure to immediate relatives of deceased persons. For more information see the fact sheet here.

Identifiers and anonymity

12. Not identified

Only use unique identifiers to identify people if it is reasonably necessary to carry out your functions efficiently.

13. Anonymous

Give the person the option of receiving services from you anonymously, where this is lawful and practicable.

Transferrals and linkage

14. Controlled

An agency should not transfer health information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless they are able to rely on one of the exceptions. For further information see the fact sheet here.

15. Authorised

Only use health records linkage systems if the person has provided their express consent.

Mandatory Notification of Data Breach Scheme

The Mandatory Notification of Data Breach Scheme (the MNDB Scheme) imposes a number of obligations on public sector agencies and their staff.

Where there are reasonable grounds to suspect that an eligible data breach may have occurred, an officer or employee of a public sector agency must report the data breach to the head of the agency. Likewise, the agency must:

- Make all reasonable efforts to **contain** the breach,
- **Assess** whether there has been unauthorised access to, or unauthorised disclosure of, personal information, or a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information within 30 days.
- **Assess** whether there is a likelihood of serious harm to any affected individual within 30 days.
- Make all reasonable attempts to **mitigate** the harm done by the suspected breach.

Where a data breach has been assessed as an eligible data breach, agencies must:

- **Notify** the Privacy Commissioner immediately, using the form approved by the Privacy Commissioner
- **Notify** affected individuals as soon as practicable.

Agencies must also maintain:

- A public data breach policy,
- A public register of data breach notifications issued by the agency.
- An internal register of eligible data breaches at the agency.

For further information about the MNDB scheme see the Mandatory Notification of Data Breach Scheme: Guide to managing data breaches in accordance with the PPIP Act.

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 fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances.