Fact Sheet May 2026

Health Privacy Principles (HPPs)

Who is this information for?	This fact sheet is designed for agencies, organisations and members of the public.
Why is this information important to them?	This fact sheet will assist with understanding about the Health Privacy Principles (HPPs) that apply to the protection of health information under the *Health Records and Information Privacy Act 2002* (HRIP Act).

The HRIP Act outlines how New South Wales (NSW) organisations[1] collect, hold or use the health information of the public of NSW. It applies to public sector agencies or a private sector person that is a health service provider[2]. The requirements for the management of health information are governed by 15 Health Privacy Principles (HPPs).

Under the HRIP Act, health information[3] means:

(a) personal information that is information or an opinion about—

(i) the physical or mental health or a disability (at any time) of an individual, or

(ii) an individual's express wishes about the future provision of health services to him or her, or

(iii) a health service provided, or to be provided, to an individual, or

(b) other personal information collected to provide, or in providing, a health service, or

(c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or

(d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or

(e) healthcare identifiers

Exemptions may apply in certain circumstances to the definition of health information or the application of the HPPs.

Information about the 15 HPPs is summarised below. In addition to the 15 HPPs there are 12 IPPs which apply under the *Privacy and Personal Information Protection Act* to govern the management of personal information.

Agencies and organisations should consult the full text of the legislation for further information and/or contact the Privacy Contact Officer for further advice about the IPPs or HPPs.

Members of the public can also contact the Privacy Contact Officer at the relevant agency or organisation or the Information and Privacy Commissioner (IPC) for further advice.

Collection

1. Lawful

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

Health information should not be collected by any unlawful means.

2. Relevant

An organisation that collects health information from an individual must take reasonable steps to ensure that the information collected is relevant, accurate, up to date, complete and not excessive, and that the collection does not unreasonably intrude into the personal affairs of the person to whom the information relates to.

3. Direct

An organisation must only collect health information from the person concerned, unless it is unreasonable or impracticable to do so.

[1] See Section 4 HRIP Act 2002

[2] See section 4 HRIP Act 2002

[3] See Section 6, HRIP Act 2002

4. Open

An organisation that collects health information about an individual from the individual must at or before the time (or if not practicable as soon as practicable after that time) that it collects the information take reasonable steps to inform the person the identity of the organisation collecting the information and how to contact it, the fact that the individual is able to request access to the information, why they are collecting their health information, what they will do with it, and who else may see it. An organisation is to inform the individual of any law that requires the collection and of any consequences that will occur if they decide not to provide their information to the organisation.

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

An organisation that holds health information must ensure the health information is stored securely, not kept any longer than necessary for the purposes of its collection, and disposed of appropriately. An organisation is to ensure that appropriate security safeguards as are reasonable in the circumstances are in place, so that the health information is protected against loss, unauthorised access, use, modification, disclosure or any other misuse.

(Note: private sector organisations should also refer to section 25 of the HRIP Act for further provisions relating to retention.)

Access and accuracy

6. Transparent

An organisation that holds health information must take reasonable steps to explain to the person whether health information is held, whether it holds health information relating to that person and if health information is held what health information is being stored, the reasons it is being used and any rights they have to access it.

7. Accessible

An organisation that holds health information must allow a person to access their health information without unreasonable delay or expense.

(Note: private sector organisations should also refer to sections 26-32 of the HRIP Act for further provisions relating to access.)

8. Correct

An organisation is to allow a person to whom the information relates, to update, correct, delete, add or amend their health information where necessary (unless an exception applies) to ensure that the health information is accurate, is being collected or used for its directly related purpose, and is relevant, up to date, complete and not misleading.

Note: private sector organisations should also refer to sections 33-37 of the HRIP Act for further provisions relating to amendment.

9. Accurate

An organisation that holds health information must not use the health information without having taken reasonable steps to ensure that the health information is relevant, up to date, accurate, complete, and not misleading.

Use

10. Limited

An organisation that holds health information must only use health information for the purpose for which it was collected or for a directly related purpose, which a person would expect. Otherwise, use of the health information for a secondary purpose, unless one the exceptions in HPP 10 applies (e.g. emergencies, threat to health or welfare, research or training etc) would generally need the consent of the individual to whom the information relates.

Disclosure

11. Limited

An organisation that holds health information must only disclose health information for the purpose for which it was collected, or for a directly related purpose that a person would expect. Otherwise, the individual to whom the information relates would generally need to provide their consent, unless one of the exceptions in HPP 11 applies (e.g. in some instances disclosure is allowed in the event of an emergency, serious threat to health or welfare, research or training etc).

Note: also see HPP 10.

Identifiers and anonymity

12. Not identified

An organisation may only identify people by using unique identifiers if it is reasonably necessary to carry out its functions efficiently.

13. Anonymous

An organisation must give the person the opportunity of receiving services from anonymously, where this is lawful and practicable.

Transferrals and linkage

14. Controlled

An organisation must only transfer health information about an individual outside New South Wales in accordance with HPP 14.

15. Authorised

An organisation must only use health records linkage systems if the person has expressly consented to this information being included (this includes disclosure of an identifier). An organisation is not required to comply with HPP 15 if the organisation is lawfully authorised not to comply, or non-compliance is otherwise permitted o the inclusion of the health information is a use of the information that complies with HPP 10I(1)(f) or HPP11(1)(f).

Other useful resources

Other resources that may be useful on this topic include:

- *Health Records and Information Privacy Act 1998*
- NSW Privacy Laws
- Fact Sheet - Information Protection Principles
- Animation - 15 principles NSW public & private sector organisations must follow to protect health information
- Fact Sheet – Statutory guidelines under the Health Records and Information Privacy Act 2002

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.