information and privacy commission new south wales

Understanding your privacy obligations – for public sector staff

fact sheet

April 2013

Under New South Wales privacy laws, public sector agencies and staff in New South Wales are responsible for protecting the privacy of personal information they collect.

The *Privacy and Personal Information Protection Act 1998* (PPIP Act) outlines the basic obligations to protect the information agencies collect about individuals. The *Health Records and Information Privacy Act 2002* (HRIP Act) relates to health information. The NSW Privacy Commissioner has the power to investigate complaints regarding privacy under these laws.

Information Protection Principles

The 12 Information Protection Principles (IPPs) are your key to the *Privacy and Personal Information Act 1998* (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.

Exemptions may apply, therefore it is suggested you contact the Privacy Contact Officer in your agency or the NSW Information and Privacy Commission for further advice.

Collection

1. Lawful – Only collect personal information for a lawful purpose, which is directly related to the agency's activities and necessary for that purpose.

2. Direct – Only collect personal information directly from the person concerned, unless it is unreasonable or impractical to do so.

3. Open – Inform the person as to why you are collecting 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 any consequences that may apply if they decide not to provide their information to you.

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

Storage

5. Secure – 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 & accuracy

6. Transparent – 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 – Allow people to access their personal information without unreasonable delay, or expense.

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

Use

9. Accurate – Make sure that the personal information is relevant and accurate before using it.

10. Limited – Only use personal information if the person has given their consent or if they were informed at the time of collection that it would be disclosed.

Disclosure

11. Restricted – Only disclose personal information with a person's consent or if the person was told at the time that it would be disclosed. 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.

12. Safeguarded – An agency cannot disclose sensitive personal information without a person's consent, for example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, health or 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.

information and privacy commission
new south wales

Health Privacy Principles

The 15 Health Privacy Principles (HPPs) are the key to the Health Records and Information Privacy Act 2002 (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. Exemptions may apply, therefore it is suggested you seek further advice from the Privacy Contact Officer in your agency or organisation or the IPC.

Collection

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

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

3. Direct – Only collect health information directly from a person concerned, unless it is unreasonable or impracticable to do so. See the handbook on Health Privacy for an explanation of "unreasonable" and "impracticable". *Visit www.ipc.nsw.gov.au*

4. Open – Inform a person as to why you are collecting 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 that will occur if they decide 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. *(Note: private sector organisations should also refer to section 25 of the HRIP Act for further provisions relating to retention).*

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

8. Correct – Allow a person to update, correct or amend their personal information where necessary. *(Note: private sector organisations should also refer to sections 33-37 of the HRIP Act for further provisions relating to amendment).*

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. Otherwise, you would generally need their consent to use the health information for a secondary purpose.

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. Otherwise, you would generally need their consent. (*Note: see HPP 10*).

Identifiers & anonymity

12. Not identified – Only identify people by using unique identifiers 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 & linkage

14. Controlled – Only transfer health information outside New South Wales in accordance with HPP 14.

15. Authorised – Only use health records linkage systems if the person has provided or expressed their consent.

For more information

Contact the Information and Privacy Commission:

freecall: 1800 472 679
email: ipcinfo@ipc.nsw.gov.au
website: www.ipc.nsw.gov.au