NSW GOVERNMENT Parliamentary Counsel's Office

Policy

Privacy Management

Policy Reference: 09/22

Approved by Parliamentary Counsel: Annette O'Callaghan, 3 March 2022

Contents

Purpose

PCO takes the privacy of its employees and the people of NSW seriously. This Privacy Management Plan has two purposes:

- to demonstrate to members of the public how the Parliamentary Counsel's Office (PCO) upholds and respects the privacy of our clients, staff and others about whom we hold personal information, and
- to act as a reference tool for employees to explain how PCO may best meet its privacy obligations under the Privacy and Personal Information Protection Act 1998 (NSW) and the Health Records and Information Privacy Act 2002 (NSW).

PCO and its privacy context

PCO drafts legislation for the Government and for non-government Members of Parliament. PCO also provides public access to legislation and provides a limited information service to the public about the status of legislation. PCO does not provide legal advice to the public. PCO is not responsible for any public registers.

As a NSW public sector agency, PCO is regulated by the *Privacy and Personal Information Protection Act 1998* (the PPIP Act) and the *Health Records and Information Privacy Act 2001* (HRIP Act).

Both Acts centre around what are termed ***privacy principles***. The PPIP Act covers personal information other than health information, and requires agencies to comply with information protection principles (IPPs). The IPPs cover the full life cycle of information, from the point of collection through to the point of disposal. They include obligations with respect to data security, data quality and rights of access and amendment to one's own personal information, as well as how personal information may be collected, used and disclosed.

Health information is regulated by a slightly different set of principles. Health information includes information about a person's disability and any health/disability services provided to them. There are 15 health privacy principles (HPPs) in the HRIP Act, with which PCO must comply. Like the IPPs, the HPPs cover the entire information life cycle but also include some additional principles with respect to anonymity, the use of unique identifiers, and the sharing of electronic health records.

There are exemptions to many of the privacy principles and the public register provisions. Exemptions can be found in the two Acts themselves, and in Regulations, Privacy Codes and Public Interest Directions. Exemptions that are relevant to PCO's work have been noted in this plan.

Both the PPIP Act and the HRIP Act contain criminal offence provisions applicable to PCO employees who use or disclose personal information or health information without authority.

Privacy Officer

The Executive Director, carries out the functions of the Privacy Officer at PCO.

Responsibilities of PCO employees

All PCO employees are required to comply with the PPIP and HRIP Acts. This plan is intended to assist employees to understand and comply with their obligations under those Acts.

WARNING: It is a criminal offence, punishable by up to two years' imprisonment, for any employee (or former employee) of PCO to intentionally use or disclose any personal information about another person, to which the employee has or had access in the exercise of his or her official functions, except as necessary for the lawful exercise of his or her official functions.

If employees are uncertain as to whether certain conduct may breach their privacy obligations, they should seek the advice of the Privacy Officer.

Definitions

collection of personal information means the way the PCO acquires the information. Collection can be by any means. Examples include: a written form, a verbal conversation, an online form, or taking a picture with a camera.

disclosure means when we provide personal information to an individual or body outside PCO.

health information is a subset of personal information that is *also* information or an opinion about:

- a person's physical or mental health or disability, or
- a health service provided, or to be provided, to a person, or
- a person's express wishes about the future provision of health services to him or her, or
- other personal information collected to provide a health service, or in providing a health service, or in connection with the donation of human tissue, or
- genetic information that is or could be predictive of the health of a person or their relatives or descendants.

holding personal information—PCO will be considered to be holding personal information if it is in the PCO's possession or control, or if it is held by a contractor or service provider on our behalf. Most of the privacy principles apply to when the PCO is holding personal information, which means we remain responsible for what our contractors or service providers do on our behalf. This means that information about our staff that is in the physical possession of GovConnectNSW may still be considered to be held by the PCO, and therefore the PCO remains responsible for how that personal information is handled.

personal information means information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Personal information can include information that is recorded (eg on paper or in a database) but also information that is not recorded (eg verbal conversations). It can even include physical things like a person's fingerprints, tissue samples or DNA. Some things are exempt from the definition of "personal information", including information about a person who has been dead for more than 30 years, and information about an individual that is contained in a document kept in a library, art gallery or museum for the purposes of reference, study or exhibition.

privacy obligations means the privacy principles and any exemptions to those principles that apply to PCO.

sensitive personal information means personal information that is also about a person's race, ethnicity, religion, sexuality, political or philosophical beliefs or membership of a trade union.

use means when PCO uses personal information for some purpose.

Types of personal and health information held by PCO

Given the nature of PCO's core business and its stakeholders, the personal and health information collected by PCO is quite limited. Examples of personal information held by PCO and managed in accordance with the PPIP and HRIP Acts are:

Employee records of PCO staff

Employment records, including records relating to the following:

- Recruitment,
- payroll, attendance and leave,
- banking details and tax file information,
- performance management,
- training,
- workers compensation,
- work health and safety,
- gender, ethnicity and disability of employees for diversity reporting purposes,
- medical conditions and illnesses,
- emergency contact (next of kin),
- secondary employment,
- conflicts of interest.

GovConnectNSW, an outsourced service provider under a contract managed by the Department of Finance, Services and Innovation, manages some corporate services functions for PCO such as payroll, finance and information technology. In that capacity, GovConnectNSW holds and is responsible for more detailed personal information about PCO staff such as recruitment, payroll and leave records. The contract with GovConnectNSW (under which PCO is a beneficiary agency) contains auditable compliance requirements, including ensuring that GovConnectNSW complies with the PPIP Act.

Contact details

Contact details for people external to PCO, including the following:

- government agency CEOs and instructing officers,
- Members of Parliament and their key staff contacts,
- people who contact PCO seeking information on legislation.

How the Information Protection Principles (IPPs) and Health Privacy Principles (HPPs) apply to PCO

1. Lawful collection of personal and health information (IPP 1 and HPP 1)

We will only collect personal and health information:

- by lawful means, and
- for a lawful purpose that is directly related to one of our functions, and
- where the information is reasonably necessary for that lawful purpose.

Example—when designing a survey or a form directed to PCO staff ask yourself "do we really need each bit of this information to achieve this function?"

This does not apply to:

- unsolicited personal or health information, or
- personal information we collected before 1 July 2000, or
- health information we collected before 1 September 2004.

2. The sources of the personal and health information we collect (IPP 2 and HPP 3)

We often collect personal information directly from the person involved.

We collect health information directly form the person concerned unless:

- it is reasonable or impractical to do so, and
- is collected in accordance with any relevant guidelines issued by the Privacy Commissioner.

Examples—Generally, if we need information about Sue, we will ask Sue herself and not Jim. However, if Sue and Jim are colleagues visiting the office and Sue has fainted, is OK for the first aid officer to ask Jim for some health information about Sue, such as "do you know if she is diabetic?" because it is unreasonable and impractical to ask Sue directly.

This does not apply to health information that is unsolicited or that we collected before 1 September 2004.

3. Notification when collecting personal and health information (IPP 3 and HPP 4)

When collecting personal information about an individual from that individual, we will take reasonable steps to inform the person as soon as it is practical about the following:

- the purpose for which their information is being collected,
- the persons to whom it would usually be disclosed,
- how they can request to access it,
- any law that requires the information to be collected,
- the main consequences (if any) for them if the information is not provided.

Example—if collecting personal information by way of a form, that form may contain a Privacy Notice outlining how the information will be used or to whom it will be disclosed.

Generally, we must try harder to notify people when we are collecting health information.

If we are collecting health information from someone other than the person that the information relates to, we will take reasonable steps to ensure that the individual is generally aware of these matters.

This requirement does not apply:

- to health information we collected before 1 September 2004, or
- if the individual to whom the health information relates has expressly consented to us not complying, or
- if other legislation permits or requires non-compliance, or we are otherwise lawfully authorised or required not to comply, or
- if compliance would pose a serious threat to the life or health of any individual.

4. Relevance of the personal and health information we collect (IPP 4 and HPP 2)

We only collect personal and health information that is relevant and accurate, is not excessive and does not unreasonably intrude into a person's personal affairs.

This does not apply:

- if other legislation permits or requires us to do otherwise, or
- to unsolicited personal or health information, or
- to personal information we collected before 1 July 2000, or
- to health information we collected before 1 September 2004.

Example—if we needed to know someone's age so that we could provide a particular service, we would ask for their year of birth or a general age bracket, rather than their exact date of birth.

5. Secure storage of personal and health information (IPP 5 and HPP 5)

We store personal information securely, protect it from unauthorised access, use, or disclosure, and ensure it is destroyed appropriately. We handle health information in the same manner unless we are lawfully authorised or required to do otherwise.

Examples—we follow good practice records management and will only provide personal information to a contractor or service provider if they really need it to do their job.

6. Transparency of personal and health information (IPP 6 and HPP 6)

We are transparent about the personal and health information we store, why it is used and people's right to access and amend it unless we are lawfully authorised or required to do otherwise.

Example—this plan is available on our website at www.pco.nsw.gov.au.

7. Access to personal and health information (IPP 7 and HPP 7)

We allow people to access their own personal and health information without unreasonable delay or expense unless we are lawfully allowed or required to do otherwise. See page 9 for information on how to access personal or health information held by PCO.

8. Alteration of personal and health information (IPP 8 and HPP 8)

We allow people to update, correct or amend their personal information where necessary unless other legislation permits or requires us to do otherwise. See page 9 for information on how to amend personal or health information held by PCO.

We allow people to have their health information updated, amended or deleted to ensure the information is accurate, relevant, up to date, complete and not misleading. People are also allowed, where reasonably practicable, to have recipients of that information told of any updates, corrections or other changes. If we disagree with the person about whether the information needs changing, we must instead allow the person to add a statement to our records.

We are not required to comply with this principle if other legislation permits or requires non-compliance, or we are otherwise lawfully authorised or required not to comply with it.

Example—when a person calls to notify a change of their mailing address, we will update their contact details in any contact records we hold and for no cost.

9. Accuracy of personal and health information (IPP 9 and HPP 9)

Before using personal or health information, we take reasonable steps to ensure the information is relevant, accurate and up to date.

Example—when the Grievance Officer is investigating a workplace grievance, we will give the person complained about the opportunity to correct any personal or health information we are relying on before we make our final decision.

10. Use of personal and health information (IPP 10 and HPP 10)

We will only use personal information for the purpose it was collected unless:

- the person consents to us using it for an unrelated purpose, or
- we believe on reasonable grounds that it is necessary to prevent or lessen a serious and imminent threat to anyone's life or health, or
- we are permitted or required to do so under other legislation, or
- it is reasonably necessary for us to disclose the personal information to another public sector agency to deal with or respond to correspondence from Ministers or Members of Parliament, or
- we are disclosing the personal information to a public sector agency under the administration of the Premier in order to inform the Premier about a matter.

Example: If the primary purpose of collecting a complainant's information was to investigate their workplace grievance, directly related secondary purposes within the reasonable expectations of the person for which their personal information could be used by the PCO would include independent auditing of workplace grievance files.

We may use health information for purposes other than the purpose for which it was collected:

- if the person consents to it being used for an unrelated purpose, or
- if other legislation permits or requires us to.

11. Disclosure of personal or health information (IPPs 11 and 12 and HPPs 11 and 14)

We will not disclose personal information without the person's consent unless:

- the person was informed that the information would be disclosed when it was collected, or
- we believe on reasonable grounds that it is necessary to prevent or lessen a serious and imminent threat to anyone's life or health, or
- other legislation permits or requires the disclosure, or
- it is reasonably necessary for us to disclose the personal information to another public sector agency to deal with or respond to correspondence from Ministers or Members of Parliament, or
- we are disclosing the personal information to a public sector agency under the administration of the Premier in order to inform the Premier about a matter.

12. Transfers of health information (HPP 14)

We will not transfer health information outside of New South Wales unless:

- the recipient of the information is subject to a law substantially similar to the HPPs, or

- the individual consents or, if it is impractical to gain consent, would likely to consent, or
- there is a relevant contract in place between the individual and the organisation or a third party, or
- transfer is for the benefit of the individual, or
- transfer is necessary to lessen or prevent a serious threat to life, health or safety of any person, or
- transfer is permitted by law.

If we do transfer health information we will take reasonable steps to ensure the information will not be held, used or disclosed by the recipient inconsistently with the HPPs.

13. Unique identifiers for health information (HPP12)

We do not identify individuals by using unique identifiers in relation to health information**.**

14. Anonymity (HPP13)

Members of the public who contact our office can remain anonymous where it is lawful and practical.

15. Use of health records linkage systems (HPP 15)

We do not use health records linkage systems.

Other general exemptions

The PPIP Act and HRIP Act do not:

- apply to information about an individual that is contained in a publicly available publication, or
- apply to information about an individual contained in a public interest disclosure within the meaning of the *Public Interest Disclosures Act 1994*, or that has been collected during an investigation arising out of a public interest disclosure, or
- affect the operation of the *Government Information (Public Access) Act 2009* (GIPA), or
- apply to information or an opinion about an individual's suitability for appointment or employment as a public sector official.

Requesting access and amendments to personal and health information

Informal request

A person wanting to access or amend their own personal or health information can request this by contacting the staff member managing their information. This request does not need to be in writing. In some situations, we may ask the person to make a formal application instead. We will tell the person how long the request is likely to take, particularly if it may take longer than first expected. We will contact the person to advise the outcome of their request. If a person is unhappy with the outcome of their information request, they can make a formal application to us.

Formal application

Formal applications to access or amend personal or health information can be made at any time. An informal request does not need to be made before a formal request is made. Formal applications must be in writing and addressed to the Privacy Officer. They can be delivered to us via email, post or in person.

Formal applications should:

- include the person's name and contact details, and
- state whether the person is making the application under the PPIP Act (personal information) or HRIPA (health information), and
- explain what personal or health information the person wants to access or amend, and
- explain how the person wants to access or have the information amended.

We will contact the person to advise how long the request is likely to take, particularly if it may take longer than expected. If a person thinks we are taking an unreasonable amount of time to respond to an application, they have the right to seek an internal review. Before seeking an internal review, we encourage people to contact our office to ask for an update or timeframe.

Limits and reasons for refusal

If we decide not to give access to or amend personal or health information, we will clearly explain our reasons. If records are requested and they are found to contain personal, health, or other confidential information about other individuals, the request is likely to be more complex and time consuming to manage. While the PPIP Act and HRIP Act give people the right to access their own information, they generally do not give a person the right to access someone else's information.

Please refer to page 5 for more information about how the IPPs and HPPs and relevant exemptions apply to the PCO.

Reviews

We encourage people to try to resolve privacy issues with us informally before going through the review process. This can be done by contacting the person or team who manages the information or lodging a complaint using our complaints process which is available on our website.

Internal review by our office

If a person considers that we have breached the PPIP Act or HRIP Act relating to their own personal or health information, they may request an internal review under the provisions of the PPIP Act. A person cannot seek an internal review for a breach of someone else's privacy unless they are an authorised representative of the other person.

Under section 53 (3) of the PPIP Act, an application for an internal review must:

- be in writing, and
- be addressed to our office (see our contact details on page 12), and
- specify an address within Australia to which we can reply, and
- be lodged within 6 months from when the applicant became aware of the conduct the subject of the application. Applications lodged after this time will be considered on a case by

case basis.

Internal review process

The Privacy Officer conducts internal reviews unless the internal review is about their conduct, in which case the Parliamentary Counsel will appoint someone else within our office to conduct the internal review. In accordance with section 54 of the PPIP Act, we will notify the Privacy Commissioner of any internal review application we receive and will comply with the other requirements of the PPIP Act in connection with our review.

Internal reviews follow the process set out in the Information and Privacy Commission NSW's Internal Review Checklist.

We aim to complete an internal review within 60 calendar days and will inform the applicant of the progress, particularly if it is likely to take longer than expected. When the internal review is complete, the Privacy Officer will notify the applicant in writing within 14 days of:

- the findings of the review, and
- the reasons for the finding, and
- any action we propose to take, and
- the reasons for the proposed action (or no action), and
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal.

If a person disagrees with the outcome of an internal review, or is not notified of an outcome within 60 days, they have the right to seek an external review.

External review by the NSW Civil and Administrative Tribunal

A person can seek an external review if they are unhappy with the outcome of an internal review that we have conducted or do not receive an outcome within 60 days. A person must seek an internal review before they have the right to seek an external review. To seek an external review a person must apply to the NSW Civil and Administrative Review Tribunal (NCAT). Generally, a person has 28 days from the date of the internal review decision to seek an external review.

For more information about seeking an external review, please contact the NCAT:

Website:	www.ncat.nsw.gov.au
Phone:	1300 006 228
Visit/post:	Level 10, John Maddison Tower 86–90 Goulburn Street Sydney NSW 2000

Strategies for implementation of the Privacy Management Plan

Staff awareness

We make sure that our staff are aware of an understand this plan, particularly how it applies to the work they do. Privacy breaches are more likely to occur when a plan is not sufficiently relevant to the work that is actually done in the agency. With this in mind, we have written this plan in a

practical way so our staff can understand what their privacy obligations are and how to manage personal and health information in their work.

We make our staff aware of their privacy obligations by publishing the plan on Gulbarra (our in-house wiki) and providing training as required. When our staff have questions about how to manage personal and health information and this plan does not directly answer them, they should consult PCO's Privacy Officer.

Public awareness

This plan explains to stakeholders how we manage personal and health information. This plan is publicly available on our website as open access information under the *Government Information (Public Access) Act 2009* (GIPA).

Legislation and other guiding material

Attention is drawn to the following legislation:

- *Anti-Discrimination Act 1977*
- *Criminal Records Act 1991*
- *Government Information (Public Access) Act 2009*
- *Health Records & Information Privacy Act 2002*
- *Ombudsman Act 1974*
- *Privacy and Personal Information Protection Act 1998*
- *Public Interest Disclosures Act 1994*
- *State Records Act 1998*
- *Workplace Surveillance Act 2005*

Other guiding material can be found on the website of the Information and Privacy Commission NSW at www.ipc.nsw.gov.au. This includes fact sheets, guides, protocols and checklists for use by public sector agencies to help them meet their privacy obligations.

Contacts

For information about privacy at PCO, please contact our office and speak to our Privacy Officer.

Executive Director
NSW Parliamentary Counsel's Office
GPO Box 4191
SYDNEY NSW 2001
Ph: (02) 9321 3333
Email: parliamentary.counsel@pco.nsw.gov.au

To contact the Information and Privacy Commission:

Free call: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Mail: GPO Box 7011, Sydney NSW 2001
Website: www.ipc.nsw.gov.au

Review of plan

This plan is reviewed every 2 years or sooner if legislative changes require it.