
Privacy Management Plan


Authorised	Tom Gellibrand, Chief Executive
Signature	
Date	27 November 2023

Table of Contents

1	Definitions	Error! Bookmark not defined.
2	Policy Statement	3
3	Who does this Policy apply to?	3
4	How INSW manages personal and health information	4
4.1	Personal information.....	4
4.2	Health information	4
4.3	Personal and health information collected and held by INSW.....	4
4.3.1	Information Protection Principles (IPPs)	5
4.3.2	How INSW applies the IPPs to its functions and activities.....	6
4.3.3	Exemptions	10
5	Data breaches involving personal information	10
6	Review rights and complaints	11
6.1	Internal review.....	11
6.2	External review	12
6.3	Informal or alternative review.....	12
7	Promotion, use and accessibility of the Plan	13
8	Other matters	13
8.1	Public registers.....	13
8.2	Offences.....	14
9	Contact details	14
10	Relevant Legislation and Documents	15

1 Policy Statement

Infrastructure NSW (**INSW**) is required to prepare and implement a privacy management plan in accordance with section 33 of the *Privacy and Personal Information Protection Act 1998* (NSW) (**Privacy Act**)

This Privacy Management Plan (**Plan**) sets out how INSW collects and manages personal and health information, in compliance with the requirements of the Privacy Act and the *Health Records and Information Privacy Act 2002* (NSW) (**Health Records Act**).

Specifically, the Plan addresses:

- a) how INSW develops policies and practices to ensure compliance with the requirements of the Privacy Act and the Health Records Act;
- b) how INSW trains its employees on those policies and practices;
- c) INSW's internal review procedures; and
- d) other matters which INSW considers relevant in relation to privacy and the protection of personal information which it holds.

This includes explaining how individuals can contact INSW to access and/or correct their personal and health information and what they can do if they feel that we have breached our obligations in respect of their information.

However, nothing in this Plan affects the operation and/or interpretation of the Privacy Act, the Health Records Act or any applicable privacy code or legislation. It does not create or alter any obligation at law which INSW may have.

2 Who does this Policy apply to?

The Privacy Act, the Health Records Act and this Plan applies to all INSW staff including its employees, consultants, and contractors. INSW will ensure that all staff are made aware of their responsibilities under the legislation, this Plan and any other applicable policy.

3 How does INSW manage personal and health information?

3.1 Personal information

Section 4 of the Privacy Act defines personal information as 'information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion'.

The Privacy Act also provides examples of the type of information that is not personal information.

For example, personal information does not include:

- information about an individual who has been dead for more than 30 years;
- information about an individual that is contained in a publicly available publication; and
- information or an opinion about an individual's suitability for appointment or employment as a public sector official.

This list is not exhaustive.

3.2 Health information

Section 6 of the Health Records Act defines health information as:

- a) personal information that is information or an opinion about:
 - the physical or mental health or a disability (at any time) of an individual;
 - an individual's express wishes about the future provision of health services to him or her; or
 - a health service provided, or to be provided, to an individual;
- b) other personal information collected to provide, or in providing, a health service;
- 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;
- 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, but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the Health Records Act generally or for the purposes of specified provisions of the Health Records Act.

3.3 Personal and health information collected and held by INSW

INSW collects and holds different kinds of personal and health information in order to conduct its functions.

Personal and health information collected by INSW about employees may include, but is not limited to, payroll information, leave data, personal contact information, accident/incident reports,

remuneration details and health information (such medical certificates, disclosures of pre-existing medical conditions, drug and alcohol tests, medical reports and workers compensation claims).

INSW also collects information about individuals obtained during tender processes, in the course of developing and managing business relationships and when people contact us with enquiries and complaints. This can include names, contact details, opinions, health conditions and illnesses, family relationships, housing or tenancy information, work history, education and criminal histories.

There is an important distinction between solicited and unsolicited information. For the purposes of the Privacy Act, personal information is not collected by a public sector agency if the receipt of the information by the agency is unsolicited.

However, personal information is held by INSW if:

- INSW is in possession or control of the information;
- the information is in the possession or control of a person employed or engaged by INSW in the course of their employment or engagement; or
- the information is contained in a State record which INSW is responsible for.

There is no distinction between solicited and unsolicited information for the *holding* of information.

Relevantly, some of the principles under the Privacy Act and Health Records Act apply to the collection of information while others apply to the holding of information.

3.3.1 Information Protection Principles (IPPs)

The Privacy Act protects personal information held by public sector agencies by means of 12 information protection principles (IPPs). The IPPs are:

Collection

1. **Lawful:** Only collect personal information for a lawful purpose, which is directly related to the agency's function or activities and necessary for that purpose.
2. **Direct:** Only collect personal information directly from the person concerned, unless they have authorised collection from someone else, or if the person is under the age of 16 and the information has been provided by a parent or guardian.
3. **Open:** Inform the person you are collecting the information from why you are collecting it, what you will do with it and who else might see it. Tell the person how they can view and correct their personal information, if the information is required by law or voluntary, and any consequences that may apply if they decide not to provide their information.
4. **Relevant:** Ensure that the personal information is relevant, accurate, complete, 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, modification or disclosure.

Access and 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 excessive 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, accurate, up to date and complete before using it.
10. **Limited:** Only use personal information for the purpose it was collected unless the person has given their consent, or the purpose of use is directly related to the purpose for which it was collected, or to prevent or lessen a serious or imminent threat to any person's health or safety.

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, if disclosure is directly related to the purpose for which the information was collected and there is no reason to believe the person would object, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent 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, 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.

The Health Records Act contains 15 principles, many of which are similar to those in the Privacy Act. Below is a summary of how INSW and its employees, consultants and contractors are to collect and manage personal and health information, in line with the Privacy Act and the Health Records Act.

3.3.2 How INSW applies the IPPs to its functions and activities

Why we collect personal and health information

We only collect personal and health information if:

- a) it is collected for a lawful purpose that is directly related to a function or activity of INSW; and
- b) the collection of the information is reasonably necessary for that purpose.

Who we collect personal and health information from

We collect personal and health information directly from the individual to whom the information relates, unless:

- a) the individual has authorised the collection of the information from someone else;
- b) in the case of information relating to a person who is under the age of 16 years, the information has been provided by a parent or guardian of the person; or
- c) in the case of health information, it is unreasonable or impracticable to do so.

Guidelines relating to privacy law in NSW can be found here:

http://www.ipc.nsw.gov.au/sites/default/files/file_manager/Fact_Sheet_privacy_20150122.pdf

Requirements when collecting personal and health information

When we collect personal and health information we must take reasonable steps to ensure that, before the information is collected or as soon as practicable after collection, the individual concerned is made aware of:

- a) the fact that the information is being collected;
- b) the purposes for which the information is being collected;
- c) the intended recipients of the information;

OFFICIAL

- d) whether the supply of the information by the individual is required by law or is voluntary, and any consequences for the individual if the information (or any part of it) is not provided;
- e) the existence of any right of access to, or correction of the information; and
- f) the name and address of the agency that is collecting the information and the agency that is to hold the information

This ensures that when people are asked to provide their personal information to INSW they are given enough information in order to exercise any rights that they may have under the Privacy Act. This could enable the person to decide not to provide the information in the first place.

Guidelines relating to the collection of health information can be found here:

<http://ipc.nsw.gov.au/health-privacy-principles-hpps-explained-members-public>

How we collect personal and health information

When we collect personal and health information we must take reasonable steps to ensure:

- a) the information collected is relevant to the purpose for which it is collected, is not excessive, and is accurate, up to date and complete; and
- b) the collection of the information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the information relates.

We must not take unreasonable methods to gather personal information.

How we store and secure personal and health information

Once we have collected personal and health information, we must ensure:

- a) the information is kept for no longer than is necessary;
- b) the information is disposed of securely;
- c) the information is protected against loss, unauthorised access, use, modification or disclosure, and against all other misuse; and
- d) if it is necessary for the information to be given to a person in connection with the provision of a service to INSW, we must take steps to prevent unauthorised use or disclosure of the information by that person.

The level of security that may be appropriate will depend on the nature of the personal and health information and the medium in which it is stored.

It is important to note that this does not mean that personal information should be destroyed or disposed of when they are no longer useful – compliance with the provisions of the *State Records Act 1998* (NSW) may be relevant.

Objective is INSW's records management system. Objective manages both physical and electronic files. A disposal schedule is applied at the file level. Access to files is based on privileges. Access is role based, hence employees are only given access if required for their role.

Transparency around the holding of personal and health information

We must be transparent about the personal and health information which we hold. We must enable any person to ascertain:

- a) whether the agency holds personal information;
- b) whether the agency holds personal information relating to that person; and
- c) if we do hold personal information relating to that person:
 - the nature of that information;
 - the main purposes for which the information is used; and
 - the person's entitlement to gain access to the information.

OFFICIAL

Access to personal and health information we hold

People have a right of access to their personal and health information. Accordingly, we must, at the request of the individual to whom the information relates and without excessive delay or expense, provide the individual with access to the information.

Before such information is provided, we must make proper enquiries to confirm the identity of the individual who has requested the information – unless an exception exists (discussed below) information must only be provided to individuals to whom the information relates.

Correction of personal and health information

We must, at the request of an individual to whom personal and health information relates, make appropriate amendments to ensure that the information which we hold is accurate, relevant, current, complete and not misleading.

Similarly, before any corrections are made we must make proper enquiries to confirm the identity of the individual who has requested the correction.

If we are not prepared to amend the information, the individual's request for an amendment should be attached to the information requested to be changed.

Maintaining accuracy of personal and health information

Before using personal and health information we must take reasonable steps to ensure that the information is relevant, accurate, current, complete and not misleading.

While it will depend on the particular circumstances, some factors which should be taken into consideration when determining what steps are reasonable include:

- a) whether the information has recently been updated;
- b) the manner in which the information was obtained;
- c) the purpose for which the information was collected;
- d) the purpose for which the information is used;
- e) the sensitivity of the information; and
- f) the effort and cost in checking the information.

What limits are there on the use of personal and health information

INSW must only use personal and health information for the purpose for which it was collected, unless:

- a) the individual consents to the use of the information for another purpose;
- b) if the information is not health information, the other purpose is directly related to the primary purpose;
- c) if the information is health information, the other purpose is directly related to the primary purpose and the individual would reasonably expect us to use the information for that other purpose; or
- d) we believe the use is necessary to prevent or lessen:
 - a serious and imminent threat to the life or health of the individual concerned or of another person; or
 - in the case of health information, a serious threat to public health or public safety.

It is important to note that use refers to the treatment and handling of personal information within INSW. It does not include disclosure to a third party.

A statutory guideline on consent relating to the use and disclosure of personal and health information can be found here:

http://www.ipc.nsw.gov.au/sites/default/files/file_manager/Consent_Fact_Sheet_Final.pdf

What limits are there on the disclosure of personal and health information

Subject to the below (special restrictions), we may only disclose personal and health information about an individual to a third party:

- a) the individual consents to the disclosure of the information for another purpose;
- b) if the information is not health information, the disclosure is directly related to the purpose for which the information was collected and we have no reason to believe that the individual concerned would object to the disclosure;
- c) if the information is not health information, the individual concerned is likely to have been aware, or has been made aware, that the information is usually disclosed to that third party;
- d) if the information is health information, the disclosure is for the purpose for which the information was collected, or it is directly related to the primary purpose, and the individual would reasonably expect us to disclose the information for that secondary purpose; or
- e) if we believe the use is necessary to prevent or lessen:
 - a serious and imminent threat to the life or health of the individual concerned or of another person; or
 - in the case of health information, a serious threat to public health or public safety.

A statutory guideline on consent relating to the use and disclosure of personal and health information can be found here:

http://www.ipc.nsw.gov.au/sites/default/files/file_manager/Consent_Fact_Sheet_Final.pdf

Special restrictions on the disclosure of personal and health information

Special restrictions apply to certain types of information. In particular, we must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership, health or sexual activities unless the disclosure is necessary to prevent a serious or imminent threat to the life or health of the individual concerned or another person.

There are also limitations on disclosure outside New South Wales or a Commonwealth agency. Relevantly, we must not disclose personal or health information to any person or body who is in a jurisdiction outside New South Wales or a Commonwealth agency unless:

- a) the individual concerned consents
- b) a privacy law which contains principles similar to the IPPs above applies in that jurisdiction;
- c) it is necessary for the performance of a contract between NSW and the individual or the performance of a contract between NSW and a third party which is in the interest of the individual;
- d) it is for the benefit of the individual, it is impracticable to obtain the consent of the individual and it is likely that the individual would have given their consent;
- e) the disclosure is permitted under a privacy code of practice;
- f) we believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;
- g) we have taken reasonable steps to ensure the information won't be held, used or disclosed by the recipient in a manner that inconsistent with the IPPs; or
- h) if it is permitted or required by legislation or any other law.

A statutory guideline on transborder disclosure can be found here:

http://www.ipc.nsw.gov.au/sites/default/files/file_manager/2016.06.30%20s19%20Transborder%20Guidance.pdf

The use of identifiers and the linkage of health records

We can only assign identifiers (e.g., numbers) about health information to individuals if it is reasonably necessary to enable us to carry out our functions efficiently. Presently we do not use unique identifiers for health information, as we do not need them to carry out our functions.

In addition, unless we have the consent of the individual, we must not include health information about an individual in a health records linkage system or disclose an identifier of an individual to any person if the purpose of the disclosure is to include health information about the individual in a health records linkage system.

3.3.3 Exemptions

Compliance with the IPPs is subject to certain exemptions. A full list of the exemptions can be found in Part 2, Division 3 of the Privacy Act and in Schedule 1 of the Health Records Act.

Some of the exemptions most relevant to INSW are:

- if the information is unsolicited information;
- if the information is collected in connection with proceedings before a court or tribunal;
- if non-compliance is necessary to assist another public sector agency that is an investigative agency in exercising its investigative functions;
- if compliance would prejudice the interests of the individual to whom the information relates;
- if we are lawfully authorised or required not to do so;
- if non-compliance is authorised or required by a subpoena, warrant or statutory notice to produce
- non-compliance is permitted (or is necessarily implied or reasonably contemplated) by another law (including the *State Records Act 1998* and the *Government Information (Public Access) Act 2009*); or
- if the information is sent between public sector agencies under the administration of the same Minister for the purposes of informing that Minister about any matter within that administration.

Importantly, the exemptions are particular to certain IPPs – some principles do not enjoy any exemptions.

4 Data breaches involving personal information

INSW is committed to protecting the personal and health information it holds and takes its data security responsibilities seriously.

From 28 November 2023, INSW is required to comply with the mandatory notification of data breach (MNDB) provisions under Part 6A of the Privacy Act. The MNDB Scheme requires all NSW public sector agencies to do the following in the event of a suspected data breach:

1. contain the breach and assess the likely severity of harm to impacted individuals;
2. if the agency assesses that the breach is likely to result in serious harm to an individual, to notify the Privacy Commissioner as well as impacted individuals; and
3. where impacted individuals cannot be identified or where it is not reasonably practical to notify them, to issue a public notification.

Agencies are also required to satisfy additional requirements relating to responsible handling of personal and health information, including a requirement to have a publicly available data breach management policy.

INSW has a Data Breach Policy (published on its website and intranet) which complies with the requirements of section 59ZD of the Privacy Act. Among other things, the Data Breach Policy sets out *how* INSW will respond to a data breach, establishes the roles and responsibilities of INSW staff in relation to data breaches, and identifies the steps INSW will take if a breach occurs. INSW also has a Data Breach Playbook which is a detailed plan outlining the steps to be taken by INSW to contain, assess, investigate, and respond to a data breach.

5 Review rights and complaints

5.1 Internal review

Individuals (including employees) who are aggrieved by our conduct relating to the collection or management of personal or health information have the right to seek an internal review of our conduct.

How to make an application

An application for review must be in writing to the Executive Director Corporate Services and be made within six months of the time the applicant first became aware of the conduct.

A review form is available on the website for the New South Wales Information and Privacy Commission (www.ipc.nsw.gov.au) and can be sent via:

Email: Privacy@infrastructure.nsw.gov.au or

Post: AON Tower, Level 27, 201 Kent Street, Sydney NSW 2000.

In appropriate circumstances, we may exercise our discretion to accept an out of time application.

How we will manage an application for review

Once a request has been made, it will be allocated to the Privacy Officer, unless the Privacy Officer was involved in the conduct which is the subject of the review – in which case the Executive Director Corporate Services will appoint an appropriate person to conduct the review.

The Privacy Officer, or another person appointed to conduct the review, will notify the Privacy Commissioner of request for a review and will keep the Privacy Commissioner informed throughout the review, including of its findings and proposed action.

While we may ask the Privacy Commissioner to undertake the internal review on our behalf, in most instances we will conduct the review internally. In any case, the Privacy Commissioner is entitled to make submissions to us regarding his or her view of the matter.

We will aim to complete the review within 60 calendar days and within 14 days of completion we will notify the applicant in writing of:

- a) the findings of the review (and the reasons for those findings);
- b) the action proposed to be taken by us (with reasons); and
- c) the right of the applicant to have those findings, and the agency's proposed action, reviewed by NSW Civil and Administrative Tribunal (NCAT) (see below).

5.2 External review

An applicant may seek an external review of our conduct relating to the collection or management of personal or health information if they have sought an internal review and either:

- a) they disagree with our decision; or
- b) they were not notified of a decision within 60 days from the date of their request for an internal review.

An application for external review can be made to NCAT. Generally, applications will need to be made within 28 days from the date of the decision of the internal review.

On reviewing the conduct, NCAT may decide not to take any action on the matter, or it may make one or more of the following orders:

- a) an order requiring INSW to pay to the applicant damages not exceeding \$40,000;
- b) an order requiring INSW to refrain from any conduct or action in contravention of an information protection principle or a privacy code of practice;
- c) an order requiring the performance of an information protection principle or a privacy code of practice;
- d) an order requiring personal information that has been disclosed to be corrected by INSW;
- e) an order requiring INSW to take specified steps to remedy any loss or damage suffered by the applicant;
- f) an order requiring INSW not to disclose personal information contained in a public register; or
- g) such ancillary orders as NCAT thinks appropriate.

For more information about seeking an external review including current forms and fees, please contact the NCAT:

Website: <http://www.ncat.nsw.gov.au/>

Phone: (02) 9377 5711

Visit/post: Level 9, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000

5.3 Informal or alternative review

Individuals aggrieved by our collection or management of personal or health information can also seek to resolve their grievances in an informal manner. This can include:

- a) contacting the Privacy Officer (Privacy@infrastructure.nsw.gov.au);
- b) making a complaint to the Privacy Commissioner;
- c) for employees, through the procedure in the INSW Grievance Policy; or
- d) for external persons, through our complaints and enquiries channels (e.g., on our website).

If an individual chooses to explore one of these options, they should be aware that the six-month limitation on internal reviews continues to run during an informal or alternative review.

6 Promotion, use and accessibility of the Plan

Initial training

At commencement or engagement with INSW, employees, contractors and consultants are informed of their responsibilities under the Privacy Act and Health Records Act and are required to complete the Confidentiality and Security of Information Agreement form on myCareer.

All employees, contractors and consultants are required to comply with INSW Code of Ethics and Conduct that sets out obligations in relation to acting honestly and with integrity, managing and disclosing conflicts of interest and maintaining confidentiality and security of information.

Ongoing training

A copy of the Plan and Privacy Policy is available to all employees on INSW's intranet page and all employees will be advised of any updates to the Plan and Privacy Policy.

Employees in positions which involve the collection and management of personal and health information will be provided with training relevant to their role.

Questions about personal and health information

Employees who are unsure about their responsibilities regarding the collection and management of personal and health information should contact the Privacy Officer or the New South Wales Information and Privacy Commission.

Distribution of information to the public

INSW may distribute information about our obligations relating to personal and health information to the public, including privacy statements on forms and information available from the New South Wales Information and Privacy Commission.

INSW's Privacy Policy, Data Breach Policy, and this Plan are available on the INSW website.

7 Other matters

7.1 Public registers

INSW is required to provide the following information to the public:

- a) a notification register of any MNDB Scheme notifications made under section 59N(2) of the Privacy Act. The information recorded in the register must be publicly available for at least 12 months after the date of publication and include the information specified under section 59O of the Privacy Act;
- b) a disclosure log of information previously released in response to formal access applications under the *Government Information (Public Access) Act 2009* (NSW) that may be of interest to other members of the public; and

- c) a register of contracts with a value of \$150,000 or more that INSW has with private sector organisations and which are required to be disclosed under the *Government Information (Public Access) Act 2009* (NSW).

7.2 Offences

Sections 62 to 68 of the Privacy Act set out several offences relating to the collection and management of personal information. For example, it is an offence to:

- a) intentionally disclose or use personal information for an unauthorised purpose;
- b) offer to supply personal information that has been disclosed unlawfully; and
- c) hinder the Privacy Commissioner or a member of employees from doing their job.

Similar offences exist in Part 8 of the Health Records Act. Under the Health Records Act, it is also an offence to prevent or attempt to prevent an individual from making or pursuing a request for access to health information, a complaint to the Privacy Commissioner or a review under the Privacy Act.

8 Contact details

Infrastructure NSW

Privacy Officer

Phone: (02) 8016 0182

Email: Privacy@infrastructure.nsw.gov.au

NSW Privacy Commissioner

NSW Privacy Commissioner

NSW Information and Privacy Commission

Office: Level 5, 47 Bridge Street, Sydney NSW 2000

Post: PO Box R232 Royal Exchange, NSW 2001

Phone: 1800 472 679

Email: ipcinfo@ipc.nsw.gov.au

Web: www.ipc.nsw.gov.au

NCAT

NSW Civil and Administrative Tribunal

Office/post: Level 9, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000

Website: <http://www.ncat.nsw.gov.au/>

Phone: (02) 9377 5711

9 Relevant Legislation and Documents

Related documents:

Privacy Policy (see link on INSW website and intranet)

Data Breach Policy (see link on INSW website and intranet)

Related legislation

Privacy and Personal Information Protection Act 1998

Health Records and Information Privacy Act 2002

Government Information (Public Access) Act 2009

Document Status

Title	
Version	2.0
Effective date	November 2023
Author	Privacy Officer
Authorised by	Executive Director, Corporate Services
Next review date	November 2025

Revision History Log

Version #	Revision Date	Author	Changes
2.0	November 2023	Privacy Officer	Update to reflect changes to the Privacy Act which introduced the Mandatory Notification of Data Breach Scheme
1.0	February 2020		