State Records NSW

Privacy Management Policy

Number	SR-P23/6	Version	1.0
Category	Policy	Subject	Governance
Issued by	Executive Director	Approval Date	05.04.2023
Authorised by	Executive Director	Issued Date	06.04.2023
Distribution	External	Review Date	05.04.2025

Purpose

The purpose of this Privacy policy is to explain how the State Records Authority NSW (State Records NSW) collects, uses, stores and discloses personal and health information in accordance with NSW privacy laws (**see Appendix 1**).

Background

The *Privacy and Personal Information Act* 1998 (PPIP Act) and the Health Records and Information Privacy Act 2002 (HRIP Act) regulate the way public sector agencies collect, store, use and disclose personal and health information. The PPIP Act protects personal information through 12 Information Protection Principles (IPPs) and the HRIP Act has 15 Health Protection Principles (HPPs).

Scope

This policy applies to:

- the personal and health information of State Records NSW employees, contractors, and consultants
- personal and health information of members of the Board of State Records Authority NSW
- personal information of members of the public who access or use our services or interactions with any other aspect of State Records NSW
- contact information of public officials collected in order to regulate recordkeeping and records management in the NSW public sector
- personal and health information in all forms of data capture and information collection, storage, analysis, use, communication, reporting and disclosure. This includes personal and health information in emails and other correspondence, spreadsheets, database applications, website, online and paper-based forms and meeting records, images, and surveillance records.

Policy

State Records NSW is committed to protecting the privacy of our stakeholders, including staff and the Board and members of the public.

State Records NSW is committed to protecting the personal and health information held in accordance with PPIP Act and HRIP Act, which require us to comply with Information and Health Privacy Principles. Further details about our obligations under PPIP Act and HRIP Act are contained in our Privacy Management Plan.

State Records NSW will not disclose personal or health information of our stakeholders without their consent unless this is permitted by legislation or court order.

State Records NSW will uphold our stakeholders' right to:

- access their personal information held by State Records NSW, without excessive delay or expense
- correct their personal information in certain circumstances (e.g. if it's inaccurate).

Duty of Confidentiality

State Records NSW employees handle, have access to and inspect the records of other NSW Government organisations. This means that they regularly have access to records that contain personal information. The State Records Act 1998 recognises this and places a special duty of confidentiality on them (**see Appendix 2**).

How State Records NSW collect personal and health information

State Records NSW collects personal and health information in order to perform its services and functions. This includes when:

- an enquiry is received
- a complaint is received about State Records NSW
- a feedback or comment is received on *State Records Act 1998, State Records Regulation 2015*, codes of best practice and standards issued under the *State Records Act 1998*
- a recordkeeping monitoring exercise is undertaken
- State Records NSW seeks voluntary completion of surveys to help identify current recordkeeping issues
- an application to work with State Records NSW
- asked to be included on our subscriber, mailing or contacts list.

For further information on how State Records NSW collects personal and health information, see our **Privacy Management Plan**. The Privacy Management Plan sets out how State Records NSW complies with the principles of the PPIP Act and the HRIP Act.

How information is managed by State Records NSW

State Records NSW may use, store and disclose personal and health information to perform its services and functions.

State Records NSW may use the information collected to:

- Promote awareness and understanding of State Records Act to NSW public offices and NSW community.
- Conduct monitoring exercise within the NSW public sector.
- Conduct or oversee reviews or complaints.
- Refer a complaint to a relevant authority.
- Advise staff and Board on recurring trends and issues.
- Educate stakeholders about particular issues through published reports, guidance or advice.

As outlined in State Records NSW's Privacy Management Plan, MHNSW also has a number of functions and obligations under the *State Records Act 1998* (SR Act).

To enable MHNSW to undertake these functions, State Records NSW may share certain types of information with MHNSW relating to Public Officers Senior Responsible Officers including:

- Name
- Title
- Organisation
- Email address
- Phone numbers

This information will be used by MHNSW workers to enable MHNSW to communicate to Public Offices regarding their obligations under the SR Act. Should SRO's not want their information shared with MHNSW they can opt out by emailing govrec@staterecords.nsw.gov.au

How to access and revise personal and health information

To access or amend your personal and/or health information that State Records NSW's hold, contact governance@staterecords.nsw.gov.au

What do I do if I believe my privacy has been breached?

If a staff member has a complaint about the conduct of State Records NSW or a member of its staff in relation to the collection, storage, use or disclosure of personal information, a written request should be sent to governance@staterecords.nsw.au so that an internal review may be undertaken.

An application for an internal review can address a breach in the IPPs, HPPs, a privacy code or the improper disclosure of personal information from a public register.

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

- Be in writing.
- Be addressed to State Records Authority NSW.
- Specify an address in Australia to which a notice may be sent
- Be lodged with State Records NSW within six months (or such later date as State Records NSW may allow) from the time the applicant first became aware of the conduct the subject of the application.
- Comply with such other requirements as may be prescribed by the regulations to the Act.

5. Roles and Responsibilities

- **The Executive Director is responsible for:**
  - overseeing the Privacy Management Plan
  - ensuring that State Records NSW complies with its obligations under the Privacy Acts
  - deciding whether to provide release personal information when a formal request is made by an individual under the PIPP Act or HRIP Act
  - making decisions regarding internal reviews if required
  - accepting the service of and responding to subpoenas, warrants and judicial orders.
- **Managers and supervisors are responsible for:**
  - ensuring their respective teams comply with their obligations under the Privacy Acts, including the IPPs and HPPs; promote the PMP to staff in their team.
- **Head of MHNSW Corporate ICT is response for:**
  - developing and maintaining cyber and information security policies; ensuring that the provision

of those policies is carried out; and notifying the Executive of issues, risks or vulnerabilities that impact information held by State Records NSW/MHNSW

- **Staff are responsible for:**
    - complying with the IPPs and HPPs when collecting, managing, using, and disclosing personal information; workers involved in contracting must ensure contractors or service providers comply with the privacy laws, noting that liability for compliance remains with State Records NSW / MHSNW

Delegations

- Instrument of Authority relating to release of information under *Government Information (Public Access) Act 2009*

Legislation

- *Government Information (Public Access) Act 2009 (NSW)*
- *Government Sector Employment Act 2013 (NSW)*
- *Health Records and Information Privacy Act 2002*
- *Independent Commission Against Corruption Act 1988*
- *Privacy and Personal Information Protection Act 1998*
- *Public Interest Disclosures Act 2013*
- *State Records Act 1998*
- *Work Health and Safety Act 2011 (NSW)*

Related Policies

- State Records NSW Code of Conduct
- NSW Government Cyber Security Policy
- MHNSW Appropriate Use of Digital Technologies Policy
- MHNSW Cyber Resilience and Information Security Policy
- MHNSW Cyber Security Incident Response Plan
- State Records NSW Records and Information Management Policy
- MHNSW User Access Control Policy

Other Related Documents

- Privacy Management Plan
- State Records NSW Collecting and managing contact information from public offices guidelines

Definitions

Collection	(of personal information) the way in which State Records NSW acquires personal or health information, which can include a written or online form, a verbal conversation, a voice recording, or a photograph.
Disclosure	(of personal information) occurs when State Records NSW makes known to an individual or entity personal or health information not previously known to them.
Health information	means information or an opinion about a person's physical or mental health or disability, or a person's express wishes about the future provision of his or her health services or a health service provided or to be provided to a person; See the definition at S6 HRIP Act.
Personal information	means 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, including such things as an individual's fingerprints, retina prints, body samples, or genetic characteristics. Exclusions to the definition of personal information are contained in s4(3) of the PPIP Act and includes health information; (see the definition at s4 PPIP Act and s4(3) PPIP Act and s5 of the HRIP Act).
Privacy principles	means the Information Protection Principles set out in Division 1 of Part 2 of the PPIP Act and Health Principles set out in Schedule 1 of the HRIP Act. The privacy principles set out the minimum standards for all NSW public sector agencies when handling personal and health information. Within these principles lawful exemptions are provided.
Privacy obligations	means the information privacy principles and any exemptions to those principles that apply to the IPC, which is a public sector agency.
Staff	means any person working in a casual, temporary, or permanent capacity in State Records NSW, including consultants, contractors, and volunteers.

Superseded Documents

This policy replaces:

- Nil

Revision History

Version	Date issued	Notes	By
1.0	06.04.2023	New policy reviewed upon establishment of State Records NSW	Content – Senior Project Officer / Governance Control – Governance Approval – Executive Director

Review Date

This policy will be reviewed on 05.04.2023 (2year intervals or as needed in accordance with regulatory changes)

Contact

governance@staterecords.nsw.gov.au / governance@mhnsw.au

Appendices

- **Appendix 1** – NSW's Privacy Laws
- **Appendix 2** – Authority's duty of confidentiality

Appendix 1 – NSW's Privacy Laws

This section contains a general summary of how State Records NSW/SLM must manage personal and health information under the PPIP Act and the HRIP Act. For more information, please refer directly to the relevant law or contact State Records NSW/SLM.

The Privacy and Personal Information Protection Act

What is personal information?

The PPIP Act defines personal information as:

Information or an opinion (including information or an opinion forming part of database and whether or not recorded in material form) about an individual whose identity is apparent or can be reasonably be ascertained from the information or opinion.

Personal information does not include information:

- Contained in a publicly available publication;
- About people who have been dead for more than 30 years; and
- About individuals' suitability for public sector employment.

Health information is generally excluded here as it is covered by the HRIP Act.

The PPIP Act also allows for a number of exceptions relating to law enforcement agencies.

What are the Information Protection Principles?

The PPIP Act sets out the 12 Information Protection Principles (IPPs) in sections 8-19. A brief summary of the IPPs is listed below. For a complete description please see the PPIP Act itself or 'A Guide to the Information Protection Principles' published by Privacy NSW.

Collection

i. 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.

ii. 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.

iii. 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.

iv. 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

v. 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

vi. 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.

vii. Accessible: Allow people to access their personal information without excessive delay or expense.

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

Use

ix. Accurate: Make sure that the personal information is relevant, accurate, up to date and complete before using it.

x. 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

xi. 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.

xii. 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.

Privacy Codes of Practice

Under the PRIP Act, a privacy code of practice is a statement of how an agency proposes to depart from the IPPs or the public register provisions of the PRIP Act. A privacy code of practice can substitute for compliance with the IPPs.

Public Registers

A public sector agency that keeps a public register cannot disclose personal information except for the purposes for which the register exists. The PRIP Act also introduces a right enabling people to have personal details removed or hidden from view in certain circumstances.

Offences

Offences can be found in Part 8 of the PPIP Act.

It is an offence for State Records NSW/SLM to:

- Intentionally disclose or use personal information accessed as a part of our work for an unauthorised purpose;
- Offer to supply personal information that has been disclosed unlawfully; and
- Hinder the Privacy Commissioner or a staff member from doing their job.

Health Records and Information Privacy Act

What is health information?

Health information is a more specific type of personal information and is defined in s6 of the HRIP Act. Health information can include information about a person's physical or mental health, such as a psychological report, blood test, an X-ray, or information about a person's medical appointment. It can also include personal information that is collected to provide to a health service, such as a name and contact

number on a medical record.

What are the Health Protection Principles?

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. The HRIP Act sets out the 15 Health Protection Principles (HPPs) in Schedule 1. A brief summary of the HPPs is listed below. For a complete description please see the HRIP Act itself or 'A Guide to the Health Protection Principles' published by Privacy NSW.

Collection

i. 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.

ii. 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.

iii. Direct: Only collect health information from the person concerned unless it is unreasonable or impracticable to do so.

iv. 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

v. 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

vi. 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.

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

viii. Correct: Allow a person to update, correct or amend their personal information where necessary.

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

Use

x. 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.

Disclosure

xi. 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 and anonymity

xii. Not identified: Only identify people by using unique identifiers if it is reasonably necessary to carry out your functions efficiently.

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

Transferrals and linkage

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

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

Offences

Offences can be found in Part 8 of the HRIP Act. It is an offence for State Records NSW/SLM to:

- Intentionally disclose or use any health information about an individual to which the employee has or had access to in the exercise of his or her official functions;
- Offer to supply health information that has been disclosed unlawfully;
- Attempt to persuade an individual to refrain from making or to withdraw an application pursuing a request for access to health information or a complaint to the Privacy Commissioner or Tribunal; and
- By threat, intimidation, or false representation require another person to give consent or to do, without consent, an act for which consent is required.

Appendix 2 – Authority's duty of confidentiality

Section 73 of the SR Act states:

(1) A person who acquires information in the exercise of functions under this Act must not directly or indirectly make a record of the information or divulge it to another person except in the exercise of functions under this Act.

(2) It is not an offence under subsection (1) if, in legal proceedings, a person:

(a) discloses information in answer to a question that the person is compellable to answer, or

(b) produces a document or other thing that the person is compellable to produce.

(3) The provisions of any other Act imposing restrictions or obligations on a person as to secrecy or disclosure of information acquired during the administration of that Act extend to apply to a person who, in the exercise of functions under this Act, gains access to that information as a result of the information having been acquired during the administration of the other Act. For that purpose, the person who gains access to the information during the administration of this Act taken to be a person engaged in the administration of the other Act.

(4) This section does not prevent or otherwise affect:

(a) the giving of access to records under Part 6 (Public access to State records after 30 years), or

(b) the preparation and dissemination of guides and finding aids.

(5) This section does not apply to the divulging of information to, or to the production of any document or other thing to, any of the following:

(a) the Independent Commission Against Corruption,

(b) the National Crime Authority,

(c) the New South Wales Crime Commission,

(d) the Ombudsman,

(e) any other person prescribed for the purposes of this section