Independent
Review Office

Privacy Management Plan

December 2023

Contents

Document Data

Policy Owner	Independent Review Officer
Compliance required by	All staff, contractors
Approved by	Independent Review Officer
Date created	Nov 2021
Next review due	Dec 2024
Drivers	*Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) Section 33 *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act)
Reference	NSW Treasury Risk Management Toolkit for NSW Public Sector Agencies
Contact officer	Principal Policy Officer
Compliance assurance	Incident monitoring, annual reporting
Policy location	On the IRO website at https://iro.nsw.gov.au/privacy-statement

Revision History

Version	Approved by	Amendment notes
V1 Nov 2021	-	Draft
V2 Feb 2022	Executive	Updates made in response to feedback provided by the Information and Privacy Commission NSW
V3 Dec 2023	Executive	New section added on NSW Mandatory Notification of Data Breach Scheme (MNDB) which commenced on 28 November 2023

1. Privacy Management Plan overview

1.1 Purpose

The purpose of the Privacy Management Plan (PMP) is to explain how the Office of the Independent Review Officer (IRO) manages personal and health information in accordance with NSW privacy laws. This includes:

Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act)

Health Records and Information Privacy Act 2002 (NSW) (HRIP Act)

The PMP also explains who you should contact with questions about the information collected and retained by the IRO, how to access and amend your stored information and what to do if the IRO may have breached the PPIP or HRIP Acts.

In addition, the PMP is used to train the IRO's staff about how to deal with personal information. This helps to ensure that the IRO complies with the PPIP Act, the HRIP Act and the *Government Information (Public Access) Act 2009* (GIPA Act).

The IRO promotes the principles of the PMP through its Executive and staff.

The IRO Executive reinforces transparency and compliance with the PPIP and HRIP Acts by:

- endorsing this PMP and making it publicly available on its website
- identifying privacy issues when implementing new systems, and
- ensuring all staff are aware of sound privacy management practices.

The IRO ensures its staff are aware of their privacy obligations by:

- publishing the PMP in a prominent place on its website
- including the PMP as part of new starter induction and offering training as required, and
- highlighting and promoting the PMP at least once a year (e.g. during Privacy Awareness Week).

When staff members have questions about how to manage personal and health information under the PMP, they may consult the IRO Privacy Officers.

1.2 What the plan covers

This PMP includes requirements outlined in section 33(2) of the PPIP Act. The plan:

- sets out our policies and practices for ensuring compliance with privacy legislation for the benefit of both staff and members of the public
- provides our staff and contractors with the necessary knowledge and skills to manage personal and health information appropriately
- applies to our treatment of all personal and health information, whether it relates to a member of the public, an employee or any other person (such as a contractor)
- outlines our review procedures

- confirms the IRO's commitment to adhere to the principles outlined in both the PPIP Act and the HRIP Act.

2. About the IRO

The Independent Review Officer is an independent statutory office established under the *Personal Injury Commission Act 2020* (NSW) (PIC Act).

The Officer is supported by an expert team of staff employed by the IRO. The statutory functions of the IRO include to:

- find solutions for persons injured at work or in motor vehicle accidents with complaints about their insurers
- manage and administer the Independent Legal Assistance and Review Service (ILARS)
- conduct inquiries into matters arising in connection with the operation of the PIC Act and the workers compensation and motor vehicle accident legislation.

2.1 Our structure

The work of the IRO is conducted by three specialist groups:

Solutions Group

This team investigates and resolves complaints made by persons injured at work or in motor vehicle accidents about the acts or omissions of insurers.

Independent Legal Assistance and Review Service (ILARS)

ILARS is operated by Principal Lawyers, paralegals and administrative assistants who assess and manage applications for grants of funding from independent IRO Approved Lawyers. to provide legal advice and assistance to injured workers.

Strategy, Policy and Support (SPS)

This team is responsible for the development of all policy recommendations, engagement, and communication with IRO stakeholders.

2.2 Our responsibilities

2.2.1 Responsibilities of employees

All staff and contractors of the IRO are required to comply with the privacy principles set out in the PPIP Act and the HRIP Act.

If the privacy principles are breached, the IRO may face loss of reputation and trust from the community and stakeholders. Both the PPIP Act and HRIP Act contain criminal offence provisions applicable to staff and contractors who use or disclose personal information or health information without authority.

This PMP is intended to assist staff to understand and comply with their obligations under those Acts. If IRO employees feel uncertain as to whether certain conduct may breach their privacy obligations, they should seek the advice of the IRO Privacy Officers.

Employees who are suspected of conduct that would breach the privacy principles or the criminal provisions may be disciplined for a breach of the IRO Code of Ethics and Conduct. Suspected criminal conduct may result in dismissal or termination of employment and/or referral to NSW Police.

2.2.2 Responsibilities of the IRO Privacy Officers

The IRO Privacy Officers are responsible for the ongoing education of IRO staff (including any third-party service providers, consultants or contractors) about their obligations under the PPIP Act and HRIP Act, by:

- making a copy of this PMP available to all current and incoming employees, and contractors
- informing staff and contractors of any changes to the PMP
- ensuring relevant privacy documents are consolidated and made available through the IRO intranet
- supporting or arranging staff training sessions on privacy matters as required, with support from the Department of Customer Service (DCS) and Director SPS
- being available to answer any questions employees may have about their privacy obligations, and
- answering questions from members of the public or IRO employees about the content or operation of this PMP, and handling privacy related complaints.

The IRO Privacy Officers can be contacted by telephone or email:

Phone	13 94 76
Email	privacy@iro.nsw.gov.au

2.2.3 Responsibilities of the Director SPS

The Director SPS is responsible for ensuring the PMP remains up to date and supporting the IRO Privacy Officers.

The Director SPS, in accordance with clause 6 of the *Annual Reports (Departments) Regulation* 2010, will ensure that the IRO Annual Report includes:

- a statement of the action taken by the IRO in complying with the requirements of the PPIP Act and HRIP Act, and
- statistical details of any internal reviews conducted by or on behalf of the IRO.

The Director SPS will review and update this PMP:

- at least every two years
- if the IRO wishes to introduce a significant new collection, use or disclosure of personal information

- if a privacy code or a direction of the Privacy Commissioner, or the expiry of such a code or direction, significantly modifies the application of the Information Protection Principles to the operations of the IRO.

The Officer on the advice of the Director SPS, may amend this plan as necessary at any time. A revised copy of the PMP will be made available on the IRO website as soon as practicable. Any amendments will be drawn to the attention of all relevant personnel, and the NSW Privacy Commissioner will be advised of any such amendment as soon as practicable.

3. Privacy Principles

The PPIP Act and the HRIP Act contain principles about managing personal and health information which the IRO must comply with. These principles are legal obligations that describe what we must do when we collect, store, alter, use or disclose personal and health information.

The PPIP Act sets out how we must manage personal information and requires us to comply with 12 Information Protection Principles (IPPs). They are set out in **Appendix A**.

The HRIP Act sets out how we must manage health information and requires us to comply with 15 Health Privacy Principles (HPPs). The HPPs are similar to the IPPs, but in the context of the provision of health services. Even though the IRO is not a health service provider, the IRO must comply with the HPPs because it holds health information about injured people, staff and other parties.

The PMP describes how the IRO complies with the privacy principles.

There are exemptions that provide that we do not need to comply with certain IPPs and HPPs when handling personal and health information. **Appendix C** contains information about the other laws that may affect how the IRO complies with the IPPs and HPPs.

3.1 What is personal information?

Personal information is defined in section 4 of the PPIP Act 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*".

Essentially, personal information is any information or an opinion that can identify an individual.

Common examples of personal information include a person's name, date of birth, contact information, bank account details, or a claim number.

3.2 What is not personal information?

There are certain types of information that are *not* considered personal information, and these are outlined at sections 4(3) and 4A of the PPIP Act.

This means that the IPPs *do not apply* to our handling of certain types of information, including:

- 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 (for example, information provided in a newspaper or a court judgment available on the internet)
- information or an opinion about an individual's suitability for appointment or employment as a public sector official (for example, recruitment records, referee reports and performance appraisals)
- health information (health information is not 'personal information' that is covered by PIPP Act, it is covered by the HRIP Act instead).

3.3 What is health information?

Health information is a specific type of personal information that is defined in section 6 of the HRIP Act as:

- personal information that is also information or an opinion about
    - an individual's physical or mental health or disability
    - an individual's express wishes about the future provision of health services to themselves
    - a health service provided, or to be provided, to an individual
- other personal information collected to provide a health service
- other personal information about an individual collected in connection with the donation of an individual's body parts, organs or body substances
- genetic information that is or could be predictive of the health of a person or their relatives or descendants
- healthcare identifiers (for example a person's Medicare card number).

Common examples of health information include a doctor's report, an x-ray, health records or even information about a person's medical appointment.

3.4 What is <u>not</u> health information?

As with personal information, there are certain types of information which are not considered health information. These are outlined in section 5(3) of HRIP Act and include some of the types of information listed above in "What is <u>not</u> personal information?".

For example, health information about a person who has been dead for more than 30 years and some employee-related health information (such as information or an opinion about an individual's suitability for appointment or employment as a public sector official), is not considered health information.

3.5 Types of personal and health information held by the IRO

The IRO has a range of functions requiring or involving the collection and use of personal and health information about members of the public, namely injured workers and people injured in motor accidents.

We also hold information about lawyers approved by the IRO to seek grants of funding from ILARS to provide advice and assistance to injured workers (IRO Approved Lawyers).

The majority of personal and health information about IRO staff members is held by the Department of Customer Service (DCS) rather than the IRO itself, as the IRO is an agency within the DCS cluster. The IRO complies with relevant policies written by the DCS, particularly concerning human resources, finance, procurement and information technology policies. Some information, such as personal phone numbers and emergency contact details, is maintained at a local level or accessed for management purposes.

Memorandum of Understanding

The IRO and the State Insurance Regulatory Authority (SIRA) have entered into a Memorandum of Understanding (MoU) consistent with the relevant laws and privacy standards.

The MoU sets out the agreed understanding of a framework for cooperation between the IRO and SIRA in exchanging information essential for the effective and efficient performance of our respective legislative functions.

In drafting the MoU, IRO and SIRA commissioned a Privacy Impact Assessment (PIA) to evaluate the privacy impacts of sharing personal information between the two agencies. The PIA made recommendations which have been incorporated into the MoU and which are being implemented by each agency.

For further information about how DCS handles personal and health information, please visit the DCS website.

The table at **Appendix B** identifies what type of personal and health information is held by the IRO in relation to its main stakeholders. Under each category there is also a list of the main reasons why the personal information is collected.

3.6 Sources of personal and health information

The IRO collects that personal and health information from various sources including:

- members of the public
- insurers and employers
- health and allied health practitioners
- legal representatives
- NSW public sector agencies, including Ministers' offices and state-owned corporations
- private sector companies

- non-government organisations (NGOs).

3.7 Requesting access to information (IPP 7 & HPP 6)

A person has a right to request access to their own personal and health information directly to the IRO.

To access or amend your personal and/or health information you can directly contact the IRO with your request by emailing the IRO Privacy Officers at privacy@iro.nsw.gov.au.

This form of release does not require a fee or an application form. Information may be released with deletions, released subject to reasonable conditions, or released in a preferred form. We may impose conditions on the use or disclosure of information that we release in response to an informal request.

If you are not happy with the outcome of the informal request, you can make a formal application in writing under the *Government Information (Public Access) Act 2009* (NSW). Formal access applications are subject to application fees and processing charges. We will not release information if there is an overriding public interest against its disclosure.

You can make a formal application by completing a Government Information Public Access (GIPA) online application form or emailing gipa@customerservice.nsw.gov.au.

4. How we manage personal and health information

The Information Protection Principles (IPPs) and Health Privacy Principles (HPPs) set out how we must manage personal and health information.

This section provides an overview of how we comply with the IPPs and HPPs when we handle the personal and health information of members of the public, Approved Lawyers and our staff.

4.1 Collection of personal information for lawful purposes (IPP 1 & HPP 1)

We will only collect personal and health information if:

- it is for a lawful purpose that is directly related to one of our functions, and
- it is reasonably necessary for us to have the information.

We collect personal and health information in a variety of ways, including in writing (email, letter, online form) over the phone, or in person.

We only request personal and health information that is reasonably necessary for the task at hand and is required for our functions to:

- respond to information requests, answer enquiries and resolve complaints
- assess eligibility for legal funding, and
- plan and report on our service.

We avoid collecting sensitive personal information if we don't need it. Sensitive information is information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.

4.2 Direct collection (IPP 2 & HPP 3)

Wherever possible, we seek to collect personal and health information directly from the person concerned.

We will only collect information from a third party where:

- the person has authorised collection of the information from someone else
- the person is under 16 years of age – in which case we may instead collect information from the person's parent or guardian
- in the case of health information, it would be unreasonable or impracticable to collect information from an individual
- we are lawfully authorised to do this.

4.3 Requirements when collecting information (IPP 3 & HPP 4)

When collecting personal or health information from an individual, we take reasonable steps to tell them:

- the fact that the information is being collected
- what it will be used for
- what other parties (if any) that we intend will receive this type of information from us
- whether the collection is required by law or is voluntary
- what the consequences will be for the person if they do not provide the information to us
- that they have a right to access and/or correct their information held by us, and
- the name and contact details of the agency collecting the information and the agency that will hold the information.

When collecting health information about an individual from a third party, we take any reasonable steps to ensure the individual is generally aware of the notification matters above (except where doing so would threaten the life or health of any person).

Generally, we provide notification to an individual by way of a 'privacy notice' that is included on a form, web page or via recorded message at the time the personal or health information is collected, or as soon as we can afterwards.

For example, individuals submitting an online complaint form are provided with a privacy notice that details why information is collected, how it will be used and to whom it will be disclosed.

Notification is not required if the information is not collected directly from the individual, except in the case of health information. In the case of health information, we are obliged to

take reasonable steps to ensure the individual is generally aware of the notification matters except in certain circumstances.

Injured workers are advised by their Approved Lawyer of the purpose of providing their information to the IRO and the other requirements set out in IPP3 by reference to the IRO Privacy Statement.

4.4 Other requirements relating to collection of personal information (IPP 4 & HPP 2)

When collecting personal information from an individual, we will take reasonable steps to ensure that:

- we do not collect excessive personal or health information
- we do not collect personal or health information in an unreasonably intrusive manner, and
- personal and health information collected is relevant, accurate, up-to-date and complete.

To determine what might be reasonable steps, we consider:

- the purpose for which the information was collected
- the sensitivity of the information
- how many people will have access to the information
- the importance of accuracy to the proposed use
- the potential effects for the individual concerned if the information is inaccurate, out-of-date or irrelevant
- the opportunities to subsequently correct the information, and
- the ease with which agencies can check the information.

The IRO collects personal and health information only in so far as it is required for our staff to respond to information requests from individuals, to answer enquiries and resolve complaints made to our office, to assess eligibility for legal funding under the ILARS, and to plan and report on our services, including requesting information to verify the identity of individuals.

Sometimes, the IRO seeks voluntary completion of surveys on its services, advice and publications. These surveys may collect different kinds of demographic data. The IRO ensures any proposed survey or other kind of collection complies with the PPIP Act and HRIP Act.

Third party providers distribute these surveys on behalf of the IRO. The IRO ensures that these providers have appropriate privacy policies in place applying the relevant privacy principles and the information is collected in a secure environment. If you provide the IRO responses to surveys, you may decide to give us personal information, such as contact details, personal opinions, stories, experiences and backgrounds. You may also give us personal information about other people. The IRO may ask for further personal information, but only to clarify the issue being raised.

Personal and health information is received by the IRO in different forms such as through email or telephone calls.

The IRO takes steps to ensure that excessive personal and health information is not collected. We do this in the following ways:

- deciding what level of information is appropriate to be collected for each enquiry or complaint on a case-by-case basis, such that the information collected must provide enough detail to be an accurate record of the issue and assistance given, but should not contain unnecessary personal or health information
- if information is received in written form, a copy will usually be kept by the IRO in its electronic case management system. As the provision of any personal or health information is entirely voluntary, if someone provides a lot of background information, the IRO may decide not to record all of the personal or health information if it is irrelevant to the enquiry or complaint
- the IRO recognises that some people may wish to remain anonymous, and our staff will provide clear information regarding the consequences of remaining anonymous (such as not being able to properly investigate or consider a complaint where there is insufficient information provided)
- telephone calls are conducted via Skype and incoming calls through our 13 94 76 telephone number are electronically recorded; other calls (including outgoing calls) are not recorded. The IRO's telephones also display the number of the person calling, except for private or silent numbers
- where an enquiry is not able to be answered straight away, an IRO staff member will offer to take the person's contact details in order to respond at another time.

4.5 Retention and security (IPP 5 & HPP 5)

We will take reasonable security safeguards to protect personal and health information from loss, unauthorised access, use, modification or disclosure, and against all other misuse. We will ensure personal and health information is stored securely, not kept longer than necessary, and disposed of appropriately.

Where it is necessary for personal or health information to be used by a person in connection with the provision of a service to us, we will take steps to prevent unauthorised use and disclosure of that information.

We hold a large amount of personal and health information and consider the security of that information fundamental to protecting privacy. The information is kept securely to protect it against loss and unauthorised access, modification or disclosure. The information can only be accessed and used by an authorised staff member for the purpose for which it was collected and lawfully used.

Information is stored in a variety of ways, including on our databases, cloud storage, secure work devices and email accounts and by third parties.

We maintain reasonable security measures, including technical, physical and administrative actions, to protect information from unauthorised access and misuse.

Examples of such security measures include:

- restricting access to IT systems and databases to ensure that only authorised users with a clear business need can access them
- use of strong passwords for computer access and a mandatory requirement that all staff change computer access passwords on a regular basis
- print on demand (secured printing)
- implementing and maintaining **information management security policies** that are regularly reviewed and updated
- maintaining logs and audit trails
- ensuring alignment with our obligations under the NSW Cyber Security Policy
- adopting best practice in electronic and paper records management and complying with our obligations under the *State Records Act 1998* (NSW)
- **records management policies** that require information to be destroyed when no longer required and in a secure manner as appropriate (for example, using secure recycling bins and shredders)
- where it is necessary for information to be used by a third-party provider for the purposes of providing us with a service, we develop and execute contractual terms that would prevent them from unauthorised use or disclosure of information that we hold
- assessing third party supplier compliance and their security standards, and
- providing **mandatory information security awareness training** to IRO staff.

4.6 Electronic records

Once personal information is collected, it is stored and protected in the appropriate electronic records system as described in the table below.

In addition to the systems outlined below, DCS provides services for the IRO with respect to information technology, finance, procurement and HR systems and support. Each business unit has its own drive on which it stores records. Staff may also retain personal information on their secure work devices and email accounts.

This information is kept securely to protect it against loss, and unauthorised access, modification or disclosure. The information can only be accessed and used by an authorised staff member for the purpose for which it was collected and lawfully used.

System	Personal information stored
Resolve	Resolve is a Case Management System used for administering applications and grants of legal funding and recording complaints and enquiries. It contains a range of personal information including: • personal, health, and financial information of injured workers and injured persons who raise a complaint or make an enquiry of the IRO • personal, professional and financial information about approved lawyers and their employing entities (law practices) • personal, professional and financial information about medical report provider organisations and medical report providers and other health service providers • priority flags and client notes
SAP HR	SAP HR is the payroll and human resources system used by DCS and the IRO.
SAP Finance, TM1 and Prime **(maintained by DCS)**	SAP Finance, TM1 and PRIME are financial management systems which record: • employee entitlements, leave deductions, banking and tax details • name, address and payment details of non-case-related creditors, and • summaries of former employees.

4.7 Accuracy

4.7.1 Transparency (IPP 6 & HPP 6)

We enable any person to know:

- whether we hold their personal and health information
- the nature of the personal and health information

- the main purposes for which we use their personal and health information, and
- their entitlement to access their personal and health information.

We have an obligation to the community to be open about how we handle personal and health information.

Our Privacy Statement supports this Plan and sets out the types of personal and health information that we hold, the purpose for which the information is used and how individuals can access their personal and health information.

If you have any questions about the personal and health information we hold, please contact the staff member or division dealing with your information. If you are unsure about who to contact, please contact the IRO Privacy Officer.

4.7.2 Access to personal and health information (IPP 7 & HPP 7)

We allow people to access their personal and health information without excessive delay or expense. We only refuse access where authorised by law, and we will provide written reasons, if requested.

Members of the public

If you are a claimant under one of the schemes administered by IRO, you may be able to access your personal and health information by contacting the insurer who is managing your claim or an Approved Lawyer representing you.

If you wish to access the information that IRO holds about you, we encourage you to contact the staff member or IRO division holding your information.

If you do not know who to contact regarding your request, or your request has been denied, please contact the IRO Privacy Officer.

Members of staff

Staff can request access to their personnel file through their Employee Self Service. From the homepage, click on the link to the GovConnect NSW portal then click to 'Raise an Incident'. Fill in the required fields on this page using 'HR' as the Issue Type, 'HR-HR Query' as the Category and 'Personnel File' as the 'Subcategory'.

Files about disciplinary matters and grievances are confidential and access is generally provided only to the staff member to whom the file relates. Generally, staff may inspect files under supervision and will also be able to take photocopies of material on their file.

Access to information under GIPA Act

Anyone can seek access to government information that is held by us under the *Government Information (Public Access) Act 2009* (GIPA Act). There are certain considerations that are taken into account before any information is released and we may withhold the personal or health information of another person. For more information, please visit 'Accessing Information'.

If you would like to access IRO information you can contact the IRO Privacy Officers via privacy@iro.nsw.gov.au

4.8 Alterations to personal and health information (IPP 8 & HPP 8)

We will allow people to update or amend their personal and health information, to ensure it is accurate, relevant, up-to-date, complete and not misleading. Where practicable, we will notify any other recipients of any changes.

We encourage you to help us keep any information we hold about you accurate, up-to-date and complete by contacting us with updated information.

If information we hold is accurate, relevant, up-to-date, complete and not misleading but a person still insists on an amendment, we can decline to do so, but must allow the person to add a statement about the requested changes to our records.

4.8.1 Members of the public

If you do not know who to contact regarding your request, or your request has been denied, please contact the IRO Privacy Officer.

4.8.2 Members of staff

Staff can amend certain personal information using the Employee Self Service on the DCS intranet. You will need to contact People and Culture to make amendments to other personal or health information.

We encourage you to keep your information up to date and accurate, particularly information about your personal contact details and next of kin contact details so that you (or they) can be contacted in an emergency. It is also your responsibility to inform us if you wish to change your bank account details or payment details.

4.9 Use

4.9.1 Accuracy (IPP 9 & HPP 9)

Before using personal or health information, we will take reasonable steps to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading.

We will take reasonable steps to ensure that personal and health information is still relevant and accurate before we use it.

What might be considered "reasonable steps" will depend upon the circumstances, but some points to consider are:

- the context in which the information was obtained
- the purpose for which we collected the information
- the purpose for which we now want to use the information
- the sensitivity of the information
- the number of people who will have access to the information
- the potential effects for the person if the information is inaccurate or irrelevant
- any opportunities we've already given the person to correct inaccuracies, and

- the effort and cost involved in checking the information.

For example, if IRO received information from a third party that your details had changed we would contact you to verify the information with you prior to amending your information.

4.9.2 Limited Use (IPP 10 & HPP 10)

We may use personal and health information for:

- the primary purpose for which it was collected

- a directly related secondary purpose

- another purpose where it is reasonably necessary to prevent or lessen a serious and imminent threat to life or health

- another purpose for which the person has consented, or

- another purpose where permitted by law.

When we use personal and health information, it means that we use it internally within IRO. This includes the provision of information to contractors engaged by IRO to manage information on our behalf. In these circumstances, the IRO retains control over the handling and use of the information.

Generally, we only use personal and health information for the purpose for which it was collected. That purpose is set out in the privacy notice/statement that is provided when the information is collected.

A directly related secondary purpose is a purpose that is very closely related to the purpose for collection and would be the type of purpose that people would quite reasonably expect their information to be used for.

Some examples of where the law permits us to use personal or health information for another (secondary) purpose may, depending on the circumstances, include:

- quality assurance activities such as monitoring, evaluating and auditing
- work health and safety laws require that we use information to ensure the safety of our employees
- unsatisfactory professional conduct or breach of discipline
- the information relates to a person's suitability for appointment or employment as a public sector official
- finding a missing person
- preventing a serious threat to public health and safety
- research or analysis of statistics
- joint research and/or commissioned analytics with academics, the NSW Data Analytics Centre and the SafeWork NSW Centre for Work Health and Safety, and
- managing and processing enquiries, complaints and disputes.

4.10 Disclosure

4.10.1 Disclosure (IPPs 11 & 12 and HPPs 11 & 14)

We may disclose personal information if:

- 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, or

- the individual has been made aware in the privacy notice that information of this kind is usually disclosed to the recipient, or

- we reasonably believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health, or

- where the disclosure is otherwise authorised by law.

Higher protections are afforded to sensitive personal information. We can generally only disclose sensitive personal information when the person has consented to the disclosure or when it is necessary to prevent a serious and imminent threat to life or health.

We can generally disclose health information when the person has consented to the disclosure; the disclosure is directly related to the purpose for which it was collected and the individual would reasonably expect us to disclose the information for that purpose; or the disclosure is necessary to prevent or lessen a serious and imminent threat to life, health or safety.

When we disclose information, it means that we give it to a third party outside of the IRO to use the information for their own purposes. We will only do this in the circumstances outlined above, or when you have provided consent for us to do so, or it is permitted or required to by law.

For example, we provide periodic information sharing and notification of significant matters to the regulator, the State Insurance Regulatory Authority (SIRA). This is permitted under the *Personal Injury Commission Act 2020* (NSW) and we have a process in place for notifying individuals when a significant matter containing personal information is disclosed.

We may also disclose your information to the nominal insurer to resolve complaints, or for another purpose where you have given consent, or that you were previously made aware of.

Generally, we do not disclose health information outside of NSW. However, if there is a good reason to do so, we only disclose the information in accordance with the PPIP Act and the HRIP Act.

4.10.2 Identifiers (HPP 12)

We will only identify individuals by using unique identifiers if it is reasonably necessary for us to carry out our functions.

Identifiers are used to uniquely identify an individual and their health records. An identifier does not need to use a person's name as they are designed to be unique to a specific

individual (for example, a customer number, unique patient number, tax file number, or driver licence number).

For example, unique case numbers are allocated to each complaint and grant matter that the IRO receives. Date of Birth data is also used to distinguish between individuals with the same name.

Anonymity (HPP 13)

Wherever it is lawful and practicable, individuals must be given the opportunity to not identify themselves when entering into transactions with or receiving health services from an organisation.

We will give you the opportunity to transact anonymously when possible. For example, if you call us to seek general advice. However, sometimes it will be necessary for you to identify yourself so that we can help. For example, where a customer makes an enquiry about their claim.

4.10.3 Linkage of Health Records (HPP 15)

We only use health records linkage systems if an individual has provided or expressed their consent, unless the linkage is for research purposes and has been approved in accordance with statutory guidelines.

We will only use health records linkage systems when individuals have expressly consented to their information being included on such a system, or for research purposes which have been approved by an Ethics Committee and in accordance with the Statutory Guidelines on Research.

4.11 Exemptions to how we manage personal and health information

4.11.1 Specific exemptions contained in the PPIP Act and the HRIP Act

The PPIP Act and the HRIP Act provide that we need not comply with some or all of the IPPs and HPPs in certain circumstances or if certain information is collected.

Some examples of exemptions most relevant to our functions and activities include:

- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- some law enforcement, investigative and complaints handling purposes
- when authorised or required by a subpoena, warrant or statutory notice to produce
- if another law authorises or requires us not to comply
- where non-compliance is otherwise permitted, implied or reasonably contemplated by another law
- in the case of health information, to lessen or prevent a serious threat to public health or public safety
- some research purposes

- in the case of health information, compassionate reasons, in certain limited circumstances
- finding a missing person, and
- information sent between public sector agencies to transfer enquiries or to manage correspondence from a Minister or Member of Parliament.

There are no privacy codes of practice or public interest directions that allow the IRO to modify its application of the IPPs and HPPs.

In addition, the IRO does not maintain any public registers that require us to make personal information publicly available under another law.

Appendix C provides information about other applicable laws that may affect how we comply with the IPPs and HPPs.

5. Strategies for compliance and best practice

We are committed to protecting the privacy rights of members of the public, staff and Approved Lawyers.

We adopt several strategies to implement best practice principles and comply with our obligations under the PPIP Act and the HRIP Act that recognise that privacy is a shared responsibility within the IRO.

5.1 Policies and procedures

We have policies, standards and guidelines to inform and assist staff in protecting privacy. These DCS policies provide best practice guidance and practical advice on matters relating to:

- acceptable use of technology (Information and Communication Technology Acceptable Use Policy Doc 18/213936)
- dealing with confidential information (Sharing Information Securely; DCS Standard: Reducing the emailing of sensitive information and attachments – DCS Information Security Policy)
- information security
- records management (DCS Records Management Policy, NSW Cloud Policy)
- privacy breaches, and
- use of social media.

The **IRO Code of Ethics and Conduct** outlines the responsibilities of our staff in protecting privacy. All staff are provided with a copy of the Code and are regularly reminded of their obligations.

We regularly review and update our policies and procedures. For example, we update our factsheets to reflect amendments to the PPIP Act or the HRIP Act so our staff and members of the public receive accurate information about our privacy practices.

Our policies and procedures will be further strengthened over time by programs addressing audit findings around Data Governance, user access management and security controls.

Any new policy or procedure, or any policy that is changed or updated, is developed in consultation with relevant business areas and receives the endorsement of the IRO Privacy Officers, the Strategy, Policy and Support division and the Executive.

Policies and procedures, including this PMP, are communicated to staff in a range of ways, including through our intranet, printed copies and targeted and on-the-job training. They are also made available on our website.

If you require a copy of a policy or procedure that is not found on our website, please contact the IRO Privacy Officers via privacy@iro.nsw.gov.au.

5.2 Procedure for responding to a data breach

The Mandatory Notification of Data Breach Scheme was created by amendments to the *Privacy and Personal Information Protection Act 1998* (NSW) and commenced on 28 November 2023.

Please refer to Sections 7 and 8 of this PMP for more information and details on how we manage and respond to breaches.

5.3 Promoting privacy awareness

We undertake a range of initiatives to ensure our staff and members of the public are informed of our privacy practices and obligations under the PPIP Act and the HRIP Act. This also assists in identifying and mitigating risks associated with privacy and encourages best practice.

We promote this PMP, privacy awareness and compliance by:

- publishing and promoting this PMP on our intranet and website
- writing this PMP in plain English
- including mandatory privacy training in our induction program (for example, Code of Conduct and Fraud and Corruption awareness modules)
- publishing and promoting policies on our intranet
- maintaining a dedicated privacy page on our intranet that centralises all privacy resources for staff and provides information about what to do if staff are unsure about a privacy issue
- drafting and publishing privacy factsheets on our intranet to provide staff with practical guidance on privacy issues and considerations
- participating annually in Privacy Awareness Week (which includes becoming a Privacy Awareness Week Champion and conducting training seminars and campaigns for all staff during this period)
- delivering periodic face to face training across different business areas
- providing a dedicated privacy advisory service to staff

- assessing privacy impacts of new projects or processes from the outset
- endorsing a culture of good privacy practice
- letting people know about the PMP when answering questions about how the IRO manages personal and health information, and
- educating the public about their privacy rights and our obligations (for example, providing privacy information on forms that collect personal and health information).

6. Review and continuous improvement

We are committed to identifying opportunities for improvement and better practice in protecting the privacy of our staff and members of the public.

We consistently evaluate the effectiveness and appropriateness of our privacy practices, policies and procedures to ensure they remain effective and identify, evaluate and mitigate risks of potential non-compliance.

We are committed to:

- monitoring and reviewing our privacy processes regularly
- further promoting and maintaining privacy awareness and compliance
- encouraging feedback from our staff and customers on our privacy practices
- actively participating in Privacy Awareness Week and other privacy initiatives
- introducing initiatives that promote good privacy handling in our business practices (such as assessing privacy impacts of new projects or processes from the outset)
- carrying out comprehensive assessments of the risk to digital information and digital information systems that are used to process personal and health information, and
- actively promoting information security awareness to ensure all staff fully understand their responsibilities of information security compliance in their day-to-day activities.

7. If you think we have breached your privacy

We encourage you to contact us directly to resolve any concerns you have about our handling of your personal or health information.

If you think we have breached your privacy, you can discuss any concerns with the staff member dealing with your information or contact the IRO Privacy Officers via privacy@iro.nsw.gov.au

We aim to resolve issues informally with as little technicality as possible and encourage you to contact us to discuss your concerns prior to seeking an internal or external review.

7.1 Your right of internal review

You have the right to ask us for an internal review if you think we have breached your privacy.

An application for internal review must:

- be in writing
- be addressed to the Independent Review Officer, and
- specify an address in Australia where you can be contacted after the completion of the review.

To apply for an internal review, write to us at the contact details below. You may also contact us if you require assistance to request an internal review.

Alternatively, you can see the section titled 'Comment on our Services' on our website to seek an internal review.

You are able to include any relevant information with your application.

7.1.1 Process

The internal review will be conducted by a person who:

- was not involved in the conduct which is the subject of the complaint
- is a staff member of the IRO, and
- is qualified to deal with the subject matter of the complaint.

Internal review follows the process set out in the Information and Privacy Commission's internal review checklist. When the internal review is completed, you will be notified in writing of:

- the findings of the review
- the reasons for those findings
- the action we propose to take
- 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.

We are required to give a copy of your internal review request to the Privacy Commissioner.

We will also send a copy of the draft internal review report to the Privacy Commissioner and we must take into account any submissions made by the Privacy Commissioner. We will keep the Privacy Commissioner informed of the progress of the internal review and will provide a copy of the finalised internal review report.

7.1.2 Timeframes

You must lodge your request for internal review within six (6) months from the time you first become aware of the conduct that you think breached your privacy.

We may accept late applications in certain circumstances (such as if you have only become aware of your right to seek an internal review or for reasons relating to your capacity to lodge an application on time). If we do not accept your application, we will provide our reasons in writing.

We will acknowledge receipt of an internal review and will aim to:

- complete the internal review within 60 calendar days, and
- respond to you in writing within 14 calendar days of completing the internal review.

We will contact you to advise how long the review is likely to take, particularly if it may take longer than expected.

If the internal review is not completed within 60 days, you have a right to seek a review of the conduct by the NSW Civil and Administrative Tribunal (see below).

7.2 Your right to external review

You have the right to apply to the NSW Civil and Administrative Tribunal if you have sought an internal review and:

- you are not satisfied with the outcome of the internal review
- you are not satisfied with the action taken in relation to your application for internal review, and
- you do not receive an outcome of the internal review within 60 days.

Any requests for, and outcomes of, internal or external reviews will be reported in the Annual Report of the IRO (without identifying any parties).

For more information about seeking an external review, contact the NSW Civil and Administrative Tribunal on the details below:

Address	**NSW Civil and Administrative Tribunal (NCAT)** Administrative and Equal Opportunity Division Level 10, John Maddison Tower 86-90 Goulburn Street Sydney NSW 2000
Postal	PO Box K1026 Haymarket NSW 1240
Document Exchange	DX 11539 Sydney Downtown
Phone	1300 006 228
Website	www.ncat.nsw.gov.au

7.3 Complaints to the Privacy Commissioner

You have the option of complaining directly to the Privacy Commissioner if you believe that we have breached your privacy.

The Privacy Commissioner's contact details are:

Address	**Information and Privacy Commissioner** Level 15, McKell Building, 2-24 Rawson Place Haymarket NSW 2000
Email	ipcinfo@ipc.nsw.gov.au

Phone	1800 472 679
Fax	02 6446 9518
Postal	GPO Box 7011, Sydney NSW 2001
Website	www.ipc.nsw.gov.au

7.4 Contact Us

Address	**Office of the Independent Review Officer** Level 17, McKell Building 2 - 24 Rawson Place Haymarket NSW 2000
Phone	13 94 76
Email	privacy@iro.nsw.gov.au
Website	www.iro.nsw.gov.au

8. Compliance with the Mandatory Notification of Data Breach Scheme

8.1 Obligations of agencies under the Mandatory Notification of Data Breach Scheme (MNDB Scheme)

The Mandatory Notification of Data Breach Scheme (MNDB Scheme) was created by amendments to the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) and commenced on 28 November 2023.

Part 6A of the PPIP Act establishes the MNDB scheme. Under the scheme, all public sector agencies bound by the PPIP Act must notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information that are likely to result in serious harm.

Staff will be required to understand how to identify an 'eligible' data breach relating to personal or health information and how to report it.

The MNDB scheme requires agencies to have regard to any guidelines[1] issued by the NSW Privacy Commissioner when assessing a data breach.

8.2 What is an 'eligible' data breach?

A data breach occurs when personal or health information held by an agency is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure. A data breach can still occur regardless of whether there has been any disclosure of information external to the agency or publicly. For example, unauthorised access to personal information by a staff

[1] https://www.ipc.nsw.gov.au/guidelines-assessment-data-breaches-under-part-6a-ppip-act

member may amount to a data breach (provided other elements of the eligibility test have been met) even where information has not been disclosed outside of the agency.

A breach is 'eligible' if the individual(s) 'personal or health information' is disclosed, used, or lost and would likely result in 'serious harm' to the individual.

The effect on the individual(s) may include:

- physical harm, economic, financial, or material harm
- emotional or psychological harm, or
- reputational harm.

8.3 What is the role of IRO staff?

All staff are responsible for escalating to their Privacy Officer and Manager any 'eligible' data breach reported or suspected to have occurred within their team, to ensure compliance with the Mandatory Notification of Data Breach (MNDB) regulations.

Team leaders and Managers should review existing processes and identify how internal controls could be strengthened. This helps ensure that any incident is contained and reduces the risk of it happening again in the future.

8.3.1 Overview of IRO obligations

When a data breach occurs, the IRO must immediately make all reasonable efforts to contain the breach and try to reduce the likelihood that an individual will experience serious harm.

IRO then has 30 days from the date they become aware of a possible data breach to assess whether that data breach is an 'eligible' data breach. Where an agency facing a data breach does not consider that a reasonable person will conclude that the breach would likely result in serious harm, a duty to notify would not arise. This is a significant threshold to meet and accordingly not all matters will be subject to notification to the Privacy Commissioner.[2] This assessment should be carried out as expeditiously as possible. Whilst making this assessment, all reasonable attempts must be made to mitigate any harm already done.

Once the IRO decides there has been an eligible data breach, it must notify the affected individuals as soon as practicable about that breach, with limited exceptions.

Part 6A, Division 4 of the PPIP Act provides a limited number of exemptions from the requirement to notify affected individuals of an eligible data breach.

8.3.2 Prepare and publish a Data Breach Policy

Under the MNDB Scheme, the IRO is required to prepare and publish a data breach policy. A data breach policy is a documented policy or plan setting out how the IRO will respond to a

[2] As adapted from *Privacy and Personal Information Protection Amendment Bill 2022* Second Reading Speech, Attorney General Mark Speakman, accessed on 17 April 2023 at: https://www.parliament.nsw.gov.au/Hansard/Pages/HansardResult.aspx#/docid/'HANSARD-1323879322-129019'

data breach. It establishes the roles and responsibilities of IRO staff in relation to managing a breach, and the steps that IRO will follow when a breach occurs.

The IRO Data Breach Policy will be publicly accessible on the IRO website.

8.3.3 Contain and assess suspected breaches

The MNDB Scheme requires any officer or employee of the IRO with reasonable grounds to suspect that an eligible data breach has occurred to report this suspected breach to the head of the IRO, which is the Independent Review Officer.

The Independent Review Officer, or their delegate, must then carry out an assessment of whether there are reasonable grounds to believe that the suspected data breach is in fact an eligible data breach. The assessment must be completed as expeditiously as possible and within 30 days. Where the IRO determines that an eligible data breach has occurred, it must notify the Privacy Commissioner and affected individuals.

The IRO must immediately make all reasonable efforts to contain the breach and while the assessment is being conducted, make all reasonable attempts to mitigate any harm done by the breach.

8.3.4 Notification obligations

The MNDB Scheme imposes obligations on the IRO to notify both the Privacy Commissioner and affected individuals of an eligible data breach.

Once the Independent Review Officer or their delegate determines that a data breach is an 'eligible data breach' for the purposes of the Scheme, they must:

- Immediately notify the Privacy Commissioner, and
- As soon as practicable, take reasonable steps to notify affected individuals (unless an exemption applies). If the IRO is unable to directly notify any or all affected individuals, it must issue and publicise a public notification.

The MNDB Scheme requires that notifications include certain minimum details about the breach. This includes information about the IRO, the data breach, the impact on individuals and mitigation steps available to individuals.

The IRO may be exempt from notification requirements to affected individuals where:

- A breach involved multiple agencies and another agency has undertaken to provide the notification to affected individuals
- Notification would likely prejudice an investigation or court or tribunal proceedings
- Mitigation action taken by the IRO has prevented any likely serious harm resulting from the breach
- Notification would be inconsistent with a secrecy provision in another Act
- Notification would create a serious risk of harm to an individual's health or safety
- Notification would compromise the IRO's cyber security or lead to further breaches

8.4 Record keeping obligations

8.4.1 Data breach incident register

The MNDB Scheme imposes an obligation on the IRO to establish and maintain an internal register for eligible data breaches. Each eligible data breach must be entered on the register, with the following information included for each entry where practicable:

- who was notified of the breach
- when the breach was notified
- the type of breach
- details of steps taken by the IRO to mitigate harm done by the breach
- details of the actions taken to prevent future breaches
- the estimated cost of the breach

8.4.2 Notification register

The MNDB Scheme requires the IRO to maintain and publish (on its website) a public notification register for any public data breach notifications that the IRO has issued. Public notifications must be given where it is not reasonably practicable to directly notify all affected individuals. Any public notification must be kept on the register for at least 12 months from the date it was published.

The IRO must also provide the Privacy Commissioner with information on how to access the notification in the register. This requirement will generally be satisfied by the provision of a link to the website on which the notification is published.

Appendix A Information Protection Principles (IPPs)

The IPPs are copied from Part 2, Division 1 of the PPIP Act.

Principle 1 (Section 8) – Collection of personal information for lawful purposes

(1) A public sector agency must not collect personal information unless—

(a) the information is collected for a lawful purpose that is directly related to a function or activity of the agency, and

(b) the collection of the information is reasonably necessary for that purpose.

(2) A public sector agency must not collect personal information by any unlawful means.

Principle 2 (Section 9) – Collection of personal information directly from the individual

A public sector agency must, in collecting personal information, collect the information directly from the individual to whom the information relates unless—

(a) the individual has authorised collection of the information from someone else, or

(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.

Principle 3 (Section 10) Requirements when collecting personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances to ensure that, before the information is collected or as soon as practicable after collection, the individual to whom the information relates is made aware of the following—

(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,

(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, and correction of, the information,

(f) the name and address of the agency that is collecting the information and the agency that is to hold the information.

Principle 4 (Section 11) – Other requirements relating to collection of personal information

If a public sector agency collects personal information from an individual, the agency must take such steps as are reasonable in the circumstances (having regard to the purposes for which the information is collected) to ensure that—

(a) the information collected is relevant to that purpose, 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.

Principle 5 (Section 12) – Retention and security of personal information

A public sector agency that holds personal information must ensure—

(a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and

(b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and

(c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and

(d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.

Principle 6 (Section 13) – Information about and access to personal information held by agencies

A public sector agency that holds personal information must take such steps as are, in the circumstances, reasonable to enable any person to ascertain—

(a) whether the agency holds personal information, and

(b) whether the agency holds personal information relating to that person, and

(c) if the agency holds personal information relating to that person—

  (i) the nature of that information, and

  (ii) the main purposes for which the information is used, and

  (iii) that person's entitlement to gain access to the information.

Principle 7 (Section 14) – Access to personal information held by agencies

A public sector agency that holds personal information 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.

Principle 8 (Section 15) – Alteration of personal information

(1) A public sector agency that holds personal information must, at the request of the individual to whom the information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the personal information—

  (a) is accurate, and

(b) having regard to the purpose for which the information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading.

(2) If a public sector agency is not prepared to amend personal information in accordance with a request by the individual to whom the information relates, the agency must, if so requested by the individual concerned, take such steps as are reasonable to attach to the information, in such a manner as is capable of being read with the information, any statement provided by that individual of the amendment sought.

(3) If personal information is amended in accordance with this section, the individual to whom the information relates is entitled, if it is reasonably practicable, to have recipients of that information notified of the amendments made by the public sector agency.

(4) This section, and any provision of a privacy code of practice that relates to the requirements set out in this section, apply to public sector agencies despite section 25 of this Act and section 21 of the State Records Act 1998.

(5) The Privacy Commissioner's guidelines under section 36 may make provision for or with respect to requests under this section, including the way in which such a request should be made and the time within which such a request should be dealt with.

(6) In this section (and in any other provision of this Act in connection with the operation of this section), public sector agency includes a Minister and a Minister's personal staff.

Principle 9 (Section 16) – Agency must check accuracy of personal information

A public sector agency that holds personal information must not use the information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the information is proposed to be used, the information is relevant, accurate, up to date, complete and not misleading.

Principle 10 (Section 17) – Limits on use of personal information

A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless—

(a) the individual to whom the information relates has consented to the use of the information for that other purpose, or

(b) the other purpose for which the information is used is directly related to the purpose for which the information was collected, or

(c) the use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual to whom the information relates or of another person.

Principle 11 (Section 18) – Limits on disclosure of personal information

(1) A public sector agency that holds personal information must not disclose the information to a person (other than the individual to whom the information relates) or other body, whether or not such other person or body is a public sector agency, unless—

(a) the disclosure is directly related to the purpose for which the information was collected, and the agency disclosing the information has no reason to believe that the individual concerned would object to the disclosure, or

(b) the individual concerned is reasonably likely to have been aware, or has been made aware in accordance with section 10, that information of that kind is usually disclosed to that other person or body, or

(c) the agency believes on reasonable grounds 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.

(2) If personal information is disclosed in accordance with subsection (1) to a person or body that is a public sector agency, that agency must not use or disclose the information for a purpose other than the purpose for which the information was given to it.

Principle 12 (Section 19) – Special restrictions on disclosure of personal information

(1) A public sector agency must not disclose personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities unless the disclosure is necessary to prevent a serious and imminent threat to the life or health of the individual concerned or another person.

(2) A public sector agency that holds personal information about an individual must not disclose the information to any person or body who is in a jurisdiction outside New South Wales or to a Commonwealth agency unless—

(a) the public sector agency reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the information protection principles, or

(b) the individual expressly consents to the disclosure, or

(c) the disclosure is necessary for the performance of a contract between the individual and the public sector agency, or for the implementation of pre-contractual measures taken in response to the individual's request, or

(d) the disclosure is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the public sector agency and a third party, or

(e) all of the following apply—

(i) the disclosure is for the benefit of the individual,

(ii) it is impracticable to obtain the consent of the individual to that disclosure,

(iii) if it were practicable to obtain such consent, the individual would be likely to give it, or

(f) the disclosure is reasonably believed by the public sector agency to be necessary to lessen or prevent a serious and imminent threat to the life, health or safety of the individual or another person, or

(g) the public sector agency has taken reasonable steps to ensure that the information that it has disclosed will not be held, used or disclosed by the recipient of the information inconsistently with the information protection principles, or

(h) the disclosure is permitted or required by an Act (including an Act of the Commonwealth) or any other law.

Appendix B Examples of personal and health information held by the IRO

Type	Description	Category of personal and health information	Purpose of collection	Disclosure
Complaints and enquiries from injured persons or their authorised representative	IRO collects information to help resolve complaints from persons injured at work and in motor vehicle accidents	Claimant name and contact details Date of birth Details of accident Medical records of claimant Medico-legal reports Employment information (eg. payslips and tax returns) Investigation reports Claim details	To respond to enquiries and find solutions to complaints about insurers	The other party to the claim (ie insurer) to resolve complaints
Applications from Approved Lawyers for grants	IRO collects information from an injured worker's lawyer when they seek a grant of funding and at any time while the grant is open	Claimant name and contact details Date of birth Details of accident Medical records of claimant Medico-legal reports Employment information Claim details	To assess eligibility for legal funding	From a third party as part of the legal funding process. The other party to the claim (ie insurer).
Application to become an Approved Lawyer	IRO collects information from lawyers seeking to be Approved Lawyers	Lawyer's name and contact details	To assess eligibility to be an approved lawyer	

Appendix C Other applicable laws

This section contains information about the other laws that may affect how the IRO complies with the IPPs and HPPs.

Government Information (Public Access) Act 2009 (GIPA Act) and *Government Information (Public Access) Regulation 2009*

The GIPA Act provides a mechanism to access your personal information or other information. An application can be made to the IRO to access information that the IRO holds. Sometimes, this information may include personal and/or health information. If a person has applied for access to someone else's information, the IRO will take steps to consult with people who might have concerns regarding disclosure of their personal information. The IRO will provide notice of the decision to ensure that people who might want to object to the release of information have time to apply for a review of the decision to release information.

Crimes Act 1900

Under this law, the IRO must not access or interfere with data in computers or other electronic devices unless it is authorised to do so.

Government Information (Information Commissioner) Act 2009 (GIIC Act).

Under this law the Information Commissioner has the power to access government information held by other NSW public sector agencies for the purpose of conducting a review, investigation or dealing with a complaint under the GIPA Act and GIIC Act. The Information Commissioner also has the right to enter and inspect any premises of a NSW public sector agency and inspect any record.

This Act also allows the Information Commissioner to provide information to the NSW Ombudsman, the Director of Public Prosecutions, the Independent Commission Against Corruption or the Police Integrity Commission.

For further information on the operation of the GIIC Act, contact the IPC.

Privacy Act 1988 ***(Privacy Act)***

Under the Privacy Act, the Australian Information Commissioner has a number of monitoring, advice and assessment related functions regarding the handling of tax file numbers (TFNs).

The Privacy (Tax File Number) Rule 2015 (TFN Rule) issued under section 17 of the Privacy Act regulate the collection, storage, use, disclosure, security and disposal of individuals' TFN information. The TFN Rule only applies to the TFN information of individuals and does not apply to TFN information about other legal entities such as corporations, partnerships, superannuation funds and trusts.

The TFN Rule is legally binding. A breach of the TFN Rule is an interference with privacy under the Privacy Act. Individuals who consider that their TFN information has been mishandled may make a complaint to the Office of the Australian Information Commissioner (OAIC).

Data Sharing (Government Sector) Act 2015 regarding the sharing of government data between government agencies and the government Data Analytics Centre, including the sharing of de-identified personal data. Enhanced privacy safeguards apply and the usage of personal and health information must be in line with current privacy legislation.

Independent Commission Against Corruption Act 1988 regarding the misuse of information.

Public Interest Disclosures Act 1994 regarding disclosing information that might identify or tend to identify a person who has made a public interest disclosure.

State Records Act 1988 **and** ***State Records Regulation 2015*** regarding the management and destruction of records.