icare™
Insurance and Care NSW

Privacy Management Plan

28 November 2023

Contents

1. Privacy Management Plan overview

Purpose

The purpose of this Privacy Management Plan (**PMP**) is to explain how icare 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**)

This PMP explains who you should contact with questions about the information collected and held by icare, how you can access and amend information stored about you by icare and what to do if icare may have breached the PPIP or HRIP Acts.

Additionally, this PMP sets out the privacy obligations of icare and applies to the people we serve, all Employees and others who collect, use, store and disclose information on behalf of icare. icare is required to prepare and implement this PMP under the PPIP Act.

What the PMP covers

This PMP covers requirements outlined in s33(2) of the PPIP Act including:

- information about how icare develops policies and practices to ensure compliance with the PPIP Act and HRIP Act
- how icare disseminates these policies and practices within the organisation and trains its staff in their use
- icare's internal review procedures and handling of privacy complaints
- information on icare's Privacy and Data Breach Policy which contains the procedures and practices to ensure compliance with the mandatory notification of data breach scheme under Part 6A or the PPIP Act
- anything else icare considers relevant in relation to privacy and the protection of the personal and health information it holds.

Key definitions

Collection – (of personal/health information) the way in which icare acquires personal or health information, which can include a written or online form, fax, a verbal conversation, a voice recording, or a photograph.

Disclosure – (of personal/health information) occurs when icare makes known to an individual or entity personal or health information not previously known to them.

Employee – any person working in a casual, temporary, voluntary or permanent capacity at icare, including consultants and contractors.

Exemptions from compliance with Information Protection Principles (IPPs) – (general, specific and other exemptions) are provided both within the principles (and under Division 2 and Division 3 of Part 2 of the PPIP Act).

Health information – personal 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 of the HRIP Act).

Investigative agencies – any of the following: Audit Office of NSW, the Ombudsman NSW, the Independent Commission Against Corruption (ICAC) or the ICAC inspector, the Law Enforcement Conduct Commission (LECC) or the LECC Inspector and any staff of the Inspector, the Health Care Complaints Commission, the Office of the Legal Services Commissioner and Inspector of Custodial Services.

Law enforcement agencies – any of the following: the NSW Police Force or the police force of another State or Territory, the NSW Crime Commission, the Australian Federal Police, the Australian Crime Commission, the Director of Public Prosecutions of NSW or another State or Territory or of the Commonwealth, Department of Communities and Justice, NSW Sheriff's Office.

Personal information – 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) and s4A of the PPIP Act and includes health information (see the definitions at s4 of the PPIP Act and s5 of the HRIP Act and the exclusions under s4(3) and s4A of the PPIP Act).

Privacy obligations – the Privacy Principles and any exemptions to those principles that apply to icare, which is a public sector agency.

Privacy Principles – the Information Protection Principles (**IPPs**) set out in Division 1 of Part 2 of the PPIP Act and Health Privacy Principles (**HPPs**) 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 and Data Breach Policy

Separate to this PMP, icare has a Privacy and Data Breach Policy that includes icare's procedures for managing a data breach and to ensuring compliance with the mandatory notification of data breach scheme set out in Part 6A of the PPIP Act. Please refer to that Policy for further detail regarding the procedures and practices that icare uses to comply with that scheme. The Privacy and Data Breach Policy is available on icare's website at: https://www.icare.nsw.gov.au/privacy

2. About Us

icare was created on 1 September 2015 by the *State Insurance and Care Governance Act 2015* (NSW) which reformed state insurance and care schemes in NSW and included the separation of service delivery functions (icare) from regulatory roles (now performed by the State Insurance Regulatory Authority (**SIRA**)).

icare operates as a Public Financial Corporation governed by an independent Board of Directors. icare's Board is appointed by the responsible Minister, now the NSW Minister for Industrial Relations and Work Health & Safety.

icare operates the NSW Government's insurance and care schemes, which include:

- **Workers Insurance** provides workers compensation insurance to employers in NSW and their workers.
- **Lifetime Care** provides treatment, rehabilitation and care to people who have a severe injury such as a spinal cord or traumatic brain injury caused by a motor vehicle accident in NSW.
- **CTP Care** provides treatment, rehabilitation and care to people who have a motor accident injury with long-term needs and an ongoing NSW CTP claim.
- **Workers Care Program** provides treatment, rehabilitation and care to people who have a severe injury such as a spinal cord or traumatic brain injury caused by a workplace accident in NSW.
- **Dust Diseases Care** compensates and supports workers who have developed a dust disease from occupational exposure in NSW.
- **Home Building Compensation Fund** helps homeowners to rectify incomplete or defective works done by a builder or tradesperson.
- **Insurance for NSW** provides self-insurance cover to NSW Government agencies for workers compensation, public liability, property, motor vehicle and miscellaneous insurance.
- **Sporting Injuries insurance** provides cover for registered players and officials of sporting organisations that have insurance cover through icare sporting injuries insurance scheme.

More information about icare is available in icare's Agency Information Guide and at: https://www.icare.nsw.gov.au/about-us

Policy and procedure development

icare is required to set out in this PMP how policies and practices are developed to ensure compliance with the requirements of the PPIP Act and HRIP Act.

Policies and practices are developed by:

- examining changes in the legislative, policy or operational environment for their impacts on icare's privacy management
- conducting regular reviews of privacy policies and procedures
- considering the privacy implications of changes to policies and systems for any procedural changes needed.

Promoting the PMP

icare promotes the principles of this PMP through its Group Executive Team, Employees and public awareness.

Group Executive team

icare's Group Executive Team is committed to transparency and accountability in respect to compliance with the PPIP Act and the HRIP Act.

The Group Executive Team reinforces transparency and compliance with these Acts by:

- promoting this PMP
- identifying privacy issues when implementing new systems
- ensuring all Employees are aware of and trained in sound privacy management practices.

Employees

icare takes steps to ensure its Employees are aware of and comply with this PMP in all their work. Those steps include:

- publishing this PMP in a prominent place on icare's intranet and website
- including this PMP in induction packs for new Employees
- offering regular privacy training that references this PMP, such annual training or ad hoc training when required
- highlighting and promoting this PMP to Employees at least annually, such as during privacy awareness promotions
- making Employees aware of where to get additional information regarding personal and health information and privacy issues, or answers to related questions, such as by contacting their People Leader, Line 1 Risk team or icare's Privacy Team.

Public awareness

This PMP is a commitment of service to stakeholders on how icare manages personal and health information. Because it is central to how icare does business, this PMP is easy to access on the icare website and aims to be easy to understand.

icare promotes public awareness of this PMP by:

- writing it in plain English

- publishing it on icare's website at: https://www.icare.nsw.gov.au/privacy
- providing hard copies of it free of charge on request
- telling people about it when answering questions about how icare manages personal and health information.

3. What this PMP covers

This PMP addresses the management of both personal information and health information.

Personal information

'Personal information' is defined in s4 of the PPIP Act.

> *Personal information is 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.*

Personal information includes a person's name, bank account details, a photograph, or a video. Personal information also includes such things as an individual's fingerprints, retina prints, voice recordings, body samples or genetic characteristics.

Section 4 of the PPIP Act excludes certain types of information from the definition of personal information. The most significant exceptions are:

- information contained in a publicly available publication
- information about people who have been dead for more than 30 years
- information about an individual contained in a public interest disclosure
- information about an individual's suitability for public sector employment.

Recruitment records and referee reports are not personal information in circumstances where an applicant's information needs to be shared and recruitment panels) their suitability for employment during recruitment. Other recruitment information, for example a referee's personal contact details, will be maintained confidentially and will only be available to relevant staff in the recruitment process.

Section 4A of the PPIPA Act excludes health information from the definition of personal information.

Health information

Health information is governed by the HRIP Act. It is defined in s6 of the HRIP Act to mean personal information that is information or an opinion about:

- a person's physical or mental health or disability
- a person's express wishes about the future provision of health services for themselves
- a health service provided, or to be provided, to a person.

Any personal information collected for the purposes of the provision of health care will generally be ‘health information’.

Health information also includes personal information that is not itself health-related but is collected in connection with providing health services (e.g., contact details and demographic information in a health record).

There are 15 HPPs set out in Schedule 1 of the HRIP Act which govern health information in relation to public sector agencies and private sector organisations.

4. Personal and health information held by icare

Records of the people we serve and stakeholders

We normally collect personal and health information when you:

- apply for a policy of insurance
- make a claim
- become a participant in one of our schemes
- provide services to icare and the people we serve
- contact us to make an enquiry or a complaint
- visit our website or use our digital services
- are an Employee of icare or apply to become one
- interact with us in some way.

While we must collect some types of personal and health information to meet our legal obligations, we do try to limit our collection of personal and health information to what is reasonably necessary to fulfil icare’s functions. Depending on those services, or your interactions with icare, we may collect the following types of personal information:

Types of personal information collected	Kinds of personal information involved
Personal and contact details	This may include your name, address, email address, phone number, payment information and date of birth.
Australian Government related identifiers and identity documents	These may include your: • Medicare Number (for example, for Medicare Compensation Recovery) • Australian passport, driver licence, citizenship, birth, death, and marriage certificates (for example, to verify your identity) • your tax file number, such as for the purpose of meeting our obligations under the *Income Tax Assessment Act 1936* and the *Taxation Administration Act 1953*.
Health information	We collect your health information when it is relevant to icare's functions (for example, when you make a claim for an injury). This may include: • physical and mental health records • medical certificates • medical reports • details of the provision of medical and allied health care and services • future health care wishes • details of your injuries.
Financial information	This may include: • details of your employment and wages (for example, when managing your claim) • your bank details (for example, to make payments to you) • information from third parties about your credit history and insurance claims history (for example, when you are seeking a policy).
Socio-demographic information	This may include your age, gender, number of dependents, occupation, and nationality, for example when you make a claim.

Types of personal information collected	Kinds of personal information involved
Interaction information	This includes details of your interactions with us, such as when you call us, use our online services (such as making a claim or applying for a policy), make an enquiry, supply feedback or make a complaint.
Digital information	We collect information from you electronically when you use our online services (such as lodging a claim or making an enquiry). This may include: • location information (if enabled on your device) • IP address • the date and time of your visit to the site • the type of browser used. More information about the digital information we collect is available in the Website Privacy Policy.
Call recordings	Generally, we monitor and record our calls for quality training and regulatory purposes. We will let you know prior to monitoring and recording if we are doing this.
Camera surveillance	For the safety of our staff and those we serve, we use camera surveillance, such as CCTV, to monitor icare's premises.
Surveillance under Workers Compensation Legislation	On occasion we may conduct surveillance on workers compensation claimants. This surveillance is conducted in accordance with the Workers Compensation legislation and guidelines issued by the State Insurance Regulatory Authority (see Standard 25: Surveillance).
Sensitive information	On occasion, we collect and handle sensitive information. This may include: • race or ethnicity (for example we may ask you what language you speak if you request a translator to communicate with us) • criminal history, where it is relevant for our regulatory and/or legal obligations.

Types of personal information collected	Kinds of personal information involved
Information about your personal circumstances	On occasion, we may ask you to supply information about your personal circumstances so we can provide support. This may include: • information about significant life events (such as a relationship breakdown or a death in the family) • information about family and domestic violence • where you have been affected by an emergency event or a natural disaster.
Publicly available information	On occasion, we may collect and handle information that is in the public domain, such as from: • online forums, websites, Facebook, X (formerly known as Twitter), YouTube, or other social media (for example, if you use social media to make a complaint) • public registers (for example, those kept by NSW Fair Trading).
Employee records	Employee records include: • personal contact details and emergency contacts • payroll, attendance and leave records • records of gender, ethnicity and disability • medical conditions • workers compensation records • workplace health and safety records • bank account, superannuation fund and tax file numbers • performance and development records • training records • secondary employment • conflicts of interest.

How do we use your information?

We're careful about how we use your personal and health information we hold about you.

Here is a list of the ways we may use your personal and health information.

Purpose	How your information is used
Fulfilling our functions	We use your information to fulfil our functions including: • assessing, managing, and making decisions about your claim • engaging with external service providers such as professional consultants • evaluating our programs and services • undertaking research and planning new services • responding to and handling enquiries, complaints, and disputes.
Improving our business	We use your information to improve the services we provide through activities such as: • reviewing feedback from the people we serve and assessing how they use our services • testing and confirming the effectiveness of services and system enhancements • monitoring and reviewing call recordings, and other business activity for quality assurance, training, and regulatory purposes • applying data analytics to understand trends and performance.
Managing our operations	We use your information to manage our operations including to: • deliver our services • make payments for services • collect and recover money that is owed to us.
Managing security, risk, and fraud prevention	We use your information to: • prevent, detect, and investigate suspicious or fraudulent activities • monitor our properties, for example using camera surveillance to ensure the safety of our Employees and the people we serve • investigate health and safety incidents involving our Employees and the people we serve • support the management of our information security and network controls to prevent cyber-attacks, unauthorised access and other criminal or malicious activities.
To meet our legal obligations	Where required, we use your personal information to comply with the law and our regulatory obligations, including to: • confirm your identity • share relevant information with law enforcement agencies, tax authorities and other regulatory bodies

Purpose	How your information is used
	such as SIRA, the NSW Information and Privacy Commission, Independent Review Office, SafeWork NSW and NSW Fair Trading • in exceptional circumstances, icare may also need to supply your information to other bodies, for example, to the police if the information is needed for law enforcement purposes.
Managing our services	We use your information to run our services in an efficient and proper way. This includes managing our financial position, business capability and planning, testing systems and processes, as well as managing communications, corporate governance, and audit.
Performing analytics activities	Sometimes we de-identify your personal information, for example claim information, and use this to: • provide insights to other organisations and government entities (for example, to understand trends in claims) • share de-identified information with other organisations and government entities (for example, researchers).
Managing our workforce	icare uses Employee records for managing processes associated with the employment relationship with icare and general human resources management and planning functions, including: • recruitment, staff development and training • payroll, rostering, deployment, and associated processes • risk analysis and management, benchmarking, reporting, research, evaluation and analysis, auditing and quality assurance activities directly related to the icare workforce or employment at icare • workforce strategic planning, skills analysis • data analysis to develop and improve human capital services • managing performance and development • managing Employee conduct, complaints and workplace investigations • informing Employees about benefits and opportunities, for example, employment and career opportunities, learning and development, diversity and inclusion programs, and other opportunities available to employees, including dissemination of news and information directly related to employment • secondary employment

Purpose	How your information is used
	• accreditation and qualifications.

Who do we share your information with?

We may share your information with third parties for the reasons mentioned above in "How do we use your information?", or where the law otherwise allows or requires us to. We only disclose personal and health information for a purpose directly related to the reason we collected it. The types of third parties are listed below.

Type of third party	Description
Authorised third parties	We may share information with third parties where you have authorised us to do so or where we are legally required. They include: • third parties (such as legal representatives, professional consultants) • brokers • your nominated treating doctors • a person with a power of attorney • your parent or legal guardian (if you are under 16 years).
Policy holders	We share some information with policy holders (such as your employer). We only share information when we are legally authorised to do so.
Health practitioners and allied health practitioners	We may share information with those involved in your treatment and support, including: • your nominated treating doctors • other health practitioners and allied health practitioners involved in your treatment and support.
Independent experts and consultants	We may share information with independent consultants and experts who can supply advice on managing your claim, including: • injury management consultants • independent medical examiners • investigators • permanent impairment assessors.

Type of third party	Description
Third parties that can verify your information	This includes organisations that can verify information that you have supplied when applying for a policy or making a claim, including: • your employer, for example to verify your employment status, wages, and injury details • credit reporting bodies (when taking out a policy).
Our service partners	We may share your information with our service partners, external service providers and other organisations that help us to supply services. These include: • organisations that we partner with to provide services (for example, claim service providers) • external service providers that we engage to do some of our work for us, for example legal service providers and information technology and cloud service providers.
Government and law enforcement agencies	We may share your information with regulatory bodies, government agencies and law enforcement bodies to meet our legislative or regulatory obligations (for example, SIRA, SafeWork NSW, the Independent Review Officer).

Protection against intentional misuse

Both the PPIP Act and the HRIP Act contain offences for any person, such as employees, contractors and service providers, who intentionally use or disclose personal information or health information without authority. The maximum penalty for breaching is up to two years' imprisonment and/or an $11,000 fine. Where relevant, people engaging in such conduct may also be subject to claims for damages and remedies under relevant contracts, such as termination for breach.

Disclosure of Employee information to service providers and for other purposes

Employee personal information may be disclosed to service providers and contractors where necessary to support the uses outlined above for purposes directly related to the management and planning of the icare workforce.

icare may also disclose Employee personal information where authorised or required to do so by law, including:

- in response to a subpoena, summons, search warrant, or court orders
- to a law enforcement agency if there are reasonable grounds to believe that an offence has or may have been committed

- for purposes required by child protection, taxation, employment, other investigative agencies or work health and safety legislation or investigative agencies
- for purposes related to staff complaints, conduct or workplace investigation matters
- where the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of Employee or another person.

Disclosure of Employee information to members of the public

The names of Employees included in a health record or other work-related files are routinely provided to members of the public who request access to information held about them by icare.

Similarly, disclosure of an email address containing an Employee's name for work related purposes is a necessary part of routine business.

However, there may be exceptional circumstances where staff details are not disclosed to members of the public. icare can withhold staff details if there are grounds to do so under the *Government Information (Public Access) Act 2009* (NSW) (**GIPA Act**). For example, employee names are not disclosed if to do so could reasonably be expected to expose an employee to a risk of harm.

CCTV and surveillance

icare installs and maintains closed circuit television (**CCTV**) cameras on premises for a number of purposes in accordance with the *Workplace Surveillance Act 2005* (NSW), including:

- to ensure the safety and security of Employees and visitors whilst on icare premises
- to protect assets and property of icare and others
- to assist in crime prevention and aid in the investigation of criminal activity or other misconduct.

Prominent signage notifies all Employees, visitors and members of the public of the use of CCTV and that they may be under camera surveillance.

Access to the CCTV images is controlled and secure to ensure that only authorised Employees have access to any images.

5. How the Privacy Principles apply

Important note about using this Part

This part of the PMP uses plain language, not the exact wording of the law to describe the Privacy Principles and how icare Employees and contractors will comply with them. This is to make understanding our obligations easier. This

document does not cover the full complexity of the privacy laws applying to icare. It has been simplified and does not cover all exemptions or situations. If in doubt, you should always check the exact wording in the legislation and seek guidance from icare's Privacy Team. This document is an educational tool, not legal advice.

Introduction

There are 12 IPPs (Information Protection Principles) set out in in Division 1 of Part 2 of the PPIP Act and 15 HPPs (Health Privacy Principles) set out in Schedule 1 of the HRIP Act.

Our privacy obligations have been condensed into one set of 12 plain language principles to be followed by icare as follows (references in brackets are to the principles in the PPIP and HRIP Acts):

- limiting our collection of personal information (IPP 1 and HPP 1)
- anonymity and identifiers (HPPs 12, 13 and 15)
- how we collect personal information – the source (IPP 2 and HPP 3)
- how we collect personal information – the method and content (IPP 4 and HPP 2)
- notification when collecting personal information (IPP 3 and HPP 4)
- security safeguards (IPP 5 and HPP 5)
- transparency (IPP 6 and HPP 6)
- access (IPP 7 and HPP 7)
- correction (IPP 8 and HPP 8)
- accuracy (IPP 9 and HPP 9)
- use (IPP 10 and HPP 10)
- disclosure (IPPs 11 and 12, and HPPs 11 and 14).

The Privacy Principles

Principle	How we apply this principle
Limiting our collection of personal information (IPP 1 and HPP 1)	We will only collect personal 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 acquire information in many ways. Examples include: a written form, a verbal conversation, an online form, a voice recording or taking a picture or image. We won't ask for personal information unless we need it to perform one of functions or for internal administrative purposes. We will especially avoid collecting sensitive information if we don't need it.

Principle	How we apply this principle
	icare may be provided with personal information that we have not requested (unsolicited information). If we receive unsolicited information, we will determine (within a reasonable period) whether that information is directly related to our functions and reasonably necessary to perform those functions. If the information is not required, icare will take steps to destroy or de-identify the information as soon as possible. Where icare has decided to keep the information then the Privacy Principles apply.
Anonymity and Unique Identifiers (HPP 12, 13 and 15)	We will allow people to receive services from us anonymously, where lawful, secure, and practicable. People making informal enquiries or requesting general information, should not be required to identify themselves. We will only assign identifiers (such as customer numbers) to the people we serve where required. In relation to health information, we may only assign identifiers (such as a number) to an individual's health information if it is reasonably necessary. We will not include health information in a health records linkage system without a persons consent.
How we collect personal information – the source (IPP 2 and HPP 3)	We collect information directly from the person unless: • they have authorised otherwise, or • it would be unreasonable or impractical to obtain the information directly from the person. We will only collect personal and health information about a person from a third party where: • it is lawful to do so, or 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 personal information from their parent or guardian • it would be unreasonable or impracticable to collect information directly from the person. Where a person has reduced decision-making capacity we consider the NSW Privacy Commissioner's Guide – Privacy and persons with reduced decision-making capacity.
How we collect personal information – the	We will not collect personal information by unlawful means. We will not collect personal information that is intrusive or excessive.

Principle	How we apply this principle
method and content (IPP 4 and HPP 2)	We will ensure that the personal information we collect is relevant, accurate, up-to-date, complete, and not misleading.
Notification when collecting personal information (IPP 3 and HPP 4)	When collecting personal information, we will take reasonable steps at the time of collection to inform the person of: • who holds and/or has access to their personal information • what it will be used for • which organisations (if any) routinely receive this type of personal information from us • if the collection is voluntary or required by law • what the consequences are for the person if they do not provide the information to us, and • how the person can access their personal information held by us. The icare Privacy Team should review any proposals to collect new personal information or to use existing personal information for a new purpose, to ensure an adequate privacy notice is included. Privacy collection notices should be specific. If information is being collected for more than one purpose, each purpose for which the information is being collected should be specified. A privacy collection notice is not a request for consent. Its function is to tell the person providing the information of the specified matters. In the case of inbound calls to our frontline teams, a recorded message will give notice that the call may be recorded or monitored. Frontline Employees making outbound calls must provide the notice themselves. Where a person has reduced decision-making capacity we consider the NSW Privacy Commissioner's Guide - Privacy and persons with reduced decision-making capacity.
Security safeguards – storage of personal and	We will take reasonable security measures to protect personal and health information from loss, unauthorised access, modification, use or disclosure.

Principle	How we apply this principle
health information (IPP 5 and HPP 5)	We will take reasonable steps to ensure personal information is stored securely, not kept longer than necessary, and disposed of appropriately. icare protects personal information through a combination of technical security measures and practices, including: • having appropriate policies and procedures in place, including policies and procedures relating to access, use and disclosure of personal information • conducting privacy impact assessments to identify and mitigate any privacy risks to personal information • conducting security assessments to ensure that appropriate security measures and controls are in place to protect personal information • having record management systems which govern the storage, access, retention and destruction of records in accordance with our obligations under the *State Records Act 1998* (NSW) and other applicable legislation • having enforceable contracts with third party service providers that host systems and data, or collect, store and/or process information on behalf of icare • protection of information systems and data through passwords, security testing and monitoring and implementation of user rights and access controls • securely storing, transporting and destroying paper and digital records, including digital storage devices containing personal information • employee training and awareness programs.
Transparency (IPP 6 and HPP 6)	Once a person has confirmed their identity, will we take reasonable steps to allow them to find out: • whether we are likely to hold their personal information • the nature of the information we hold • the purposes for which we use personal information, and • how a person can access their own personal information. We have a broad obligation to the community to be open about how we handle personal and health information. This is different to a collection notification, which is more specific, and given to the people we serve at the time of collecting new personal information.

Principle	How we apply this principle
	This PMP will be accessible through our website. It sets out the major categories of personal information that we hold and explains our privacy obligations.
Access to information we hold (IPP 7 and HPP 7)	We will allow people to access their personal information without unreasonable delay or expense. We will only refuse access where authorised by law. If requested, we will provide written reasons for any refusal. People (whether the people we serve, Employees or other individuals) should generally be able to see what information icare holds about them without unreasonable delay. Requests can be made by phone, email or in person. Access to your own information under the PPIP Act is free. If there is any doubt about whether a request to personal information is from the individual to whom the information relates or their authorised representative, the request should be referred to the Privacy Team. In some circumstances, another law may prevent us from giving the person access to the information requested.
Correction of information we hold (IPP 8 and HPP 8)	We will allow people who have confirmed their identity to update or amend their personal information, to ensure it is accurate, relevant, up-to-date, complete, or not misleading, where appropriate.
Accuracy of information (IPP 9 and HPP 9)	Before using personal information, we will take appropriate steps to ensure that the information is relevant, accurate, up-to-date, complete, and not misleading.
Use – how we use personal and health information (IPP 10 and HPP 10)	We may use personal information for any of the following: • for the primary purpose for which it was collected • for a directly related secondary purpose • if we reasonably believe that the use is necessary to prevent or lessen a serious and imminent threat to life or health • for another purpose if the person has consented. As a general principle, we use the personal and health information we have collected only for the purpose for which it was collected, as set out in the privacy notice for that particular service.

Principle	How we apply this principle
	The primary purpose for which we use the personal information of the people we serve will be one or more of our customer service functions. We may also use information for directly related secondary purposes such as auditing, reporting or program evaluation. For example, if the primary purpose of collecting a complainant's information was to investigate the complaint, then independent auditing of our complaint-handling practices would be an acceptable use for a directly related secondary purpose. To use personal information for any other purpose, Employee's should check with the Privacy Team first. icare will generally use information with the consent of the person it relates to. However, icare may use personal information without consent in some circumstances, including: • if another law authorises, requires, implies, or reasonably contemplates the use • for some law enforcement and investigative purposes (for example, to investigate suspected fraud) • for some research purposes, subject to approval by a Human Research Ethics Committee. icare Employees and contractors should check with the Privacy Team before relying on an exemption.
Disclosure – how we disclose personal and health information (IPP 11, IPP 12 and HPP 11)	icare discloses information when it reveals the information to a person or body outside icare who did not previously know the information. Under privacy law we may disclose personal information in certain circumstances, including if one of the following apply: • the person has consented • the information is not 'health information' or 'sensitive information', and the individual has been made aware that the information is likely to be disclosed to the recipient • the information is not 'health information' or 'sensitive information', and the disclosure is directly related to the purpose for which the information was collected, and icare has no reason to believe that the individual concerned would object to the disclosure

Principle	How we apply this principle
	• the information is 'health information', and the disclosure is for the purpose for which the information was collected, or for a directly related secondary purpose within the person's reasonable expectations. We may disclose a person's 'sensitive information' only with that person's consent.
Transborder Disclosure – disclosure outside of NSW (IPP 12 and HPP 14)	We can only transfer 'health information' or disclose 'personal information' outside of NSW (including to the Commonwealth Government) if one of the following applies: • the person concerned has consented • it is necessary for the performance of a contract with (or in the interests of) the person concerned • it will benefit the person concerned, we cannot obtain their consent, but we believe the person would be likely to give their consent • we reasonably believe that the recipient of the information is subject to a law or binding scheme equivalent to the IPPs/ HPPs • we have bound the recipient by contract to privacy obligations equivalent to the IPPs/HPPs • it is permitted under another law. Under privacy law, icare may disclose personal/health information without consent in some circumstances, such as: • if we reasonably believe that the disclosure is necessary to prevent or lessen a serious and imminent threat to life or health • if it is 'health information', and we reasonably believe that the disclosure is necessary to deal with a serious threat to public health or safety • if another law authorises, requires, implies, or reasonably contemplates the disclosure • if a subpoena, warrant or 'notice to produce' requires us by law to disclose the information

Principle	How we apply this principle
	• some research purposes, subject to the Statutory Guidelines issued by the NSW Privacy Commissioner • exchanges of information which are reasonably necessary to allow agencies to deal with or respond to correspondence from Ministers or Members of Parliament, or to refer inquiries between agencies • for some law enforcement and investigative purpose (for example, to investigate suspected fraud).

6. How to access and revise your information

In most cases, you have the right to access and seek to amend (by correction, deletion, or additions) the personal and health information we hold about you, for example if you need to update your contact details.

We must provide access to or deal with your request to amend personal or health information without excessive delay or expense. We do not charge any fees to access or amend personal or health information.

You can access or request to amend your information through contact with the relevant area of icare (or your Claim Service Provider where relevant) that holds your information and through formal access applications. You also have options for requesting access to your information if your first access request has been denied.

Informal request

To access or amend your personal information, you need to contact the relevant area of icare (or your Claim Service Provider where relevant) that holds your information. You may find their contact information at Contact us.

You will need to verify your identity and, in some circumstances, for certain information, we may ask you to make a formal application.

If you need help in finding the relevant area in icare to contact, please reach out the icare Privacy Team at: privacy@icare.nsw.gov.au

Formal request

If your first request to access your personal information has been denied, you can contact the icare Privacy Team for help at: privacy@icare.nsw.gov.au

You also have the choice of making a formal application by putting your request in writing using the following forms:

- Application for access to personal and/or health information (DOCX, 0.08MB)
- Application for alteration of personal and/or health information (DOCX, 0.08MB)

7. Your rights

Privacy complaints

If you are unhappy with the way we have handled your personal or health information, we want to hear about it. We encourage to you to raise your complaint with relevant area of icare (or your Claim Service Provider where relevant) in the first instance so that, where possible, issues may be resolved quickly and simply through our complaint handling procedures. You can find more information about what happens when your make a complaint and contact information at Feedback and complaints.

If you are dissatisfied with the response you receive, you can:

- request a privacy internal review
- make a complaint to the NSW Privacy Commissioner.

Requesting an internal review

An internal review is a formal process undertaken in accordance with the privacy legislation to investigate a privacy-related complaint relating to conduct that involves personal information or health information.

To request an internal review, you can use the request for internal review form. The form itself is not mandatory, but the same information will need to be provided in writing. Supporting documentation can be attached to provide further details. A request for an internal review must be lodged with icare within 6 months (or a later date that icare may allow) from the time you first became aware of the conduct the subject of your request.

Requests for an internal review must be sent to the icare Privacy Team by:

- Email: privacy@icare.nsw.gov.au, or
- Post: icare Privacy Team, GPO Box 4052, Sydney NSW 2001

The internal review process – what you can expect

icare aims to acknowledge applications for internal reviews within 5 working days and will include an expected completion date.

icare will inform the NSW Privacy Commissioner of the application and will provide them with a copy. The NSW Privacy Commissioner is entitled to make submissions and provide relevant material for consideration if necessary.

Either the icare Principal Privacy Officer, or another person not involved in the conduct which is the subject of the complaint (that person being an employee or an officer of icare who is qualified to deal with the subject matter of the complaint), will conduct the internal review.

The internal review will, in most circumstances, be completed within 60 days of icare receiving the application

icare will follow the NSW Privacy Commissioner's internal review checklist (available at https://www.ipc.nsw.gov.au) and gives consideration to any relevant material submitted by the applicant and the NSW Privacy Commissioner.

Where appropriate, we may make recommendations as an outcome of an internal review, including one or more of the following:

- take no further action on the matter
- make a formal apology
- take appropriate remedial action, which may include payment of monetary compensation
- undertake that the conduct will not occur again
- implement administrative measures to ensure that the conduct will not occur again.

The applicant will be notified in writing of the outcome as soon as practicable, or in any event within 14 days, after the completion of the internal review, including:

- the findings of the review
- the reasons for those findings
- any action icare proposes to take
- the reasons for the proposed action (or no action)
- the applicant's entitlement to have the findings and the reasons for the findings reviewed by the NSW Civil and Administrative Tribunal (**NCAT**).

If the applicant disagrees with the outcome of an internal review or is not notified of an outcome within 60 days, the applicant has a right to seek an external review by NCAT.

To contact NCAT:

- visit NCAT's website for contact information, including information regarding making applications: http://www.ncat.nsw.gov.au
- for general enquiries telephone 1300 006 228 during business hours.

The role of the Privacy Commissioner

The PPIP Act requires that the NSW Privacy Commissioner be informed of the receipt of an application for an internal review of conduct and receive regular progress reports of the investigation. In addition, the Commissioner is entitled to make submissions in relation to an application for internal review.

In reviewing the application, icare will continue to keep the Privacy Commissioner informed of the progression and results of the internal review. Any submissions made by the Privacy Commissioner to icare will be taken into consideration when icare makes its decision.

Making a complaint to the NSW Privacy Commissioner

Privacy complaints can also be directed to the NSW Privacy Commissioner.

To contact the NSW Privacy Commissioner:

- visit the NSW Privacy Commissioner's website for contact information, including for information on making complaints: https://www.ipc.nsw.gov.au
- for general enquiries telephone 1800 472 679 during business hours.

8. Contact Us

For further information about this PMP, the personal and health information we hold, or if you have any concerns, please feel free to contact us as the following:

Email: privacy@icare.nsw.gov.au

Post: icare Privacy Team, GPO Box 4052, Sydney NSW 2001

9. Version Control and Document History

Description	
Document owner	Group Executive, Risk and Governance
Approving Authority	Group Executive, Risk and Governance
Last Approval Date	24 November 2023
Review Frequency	Annually

Version	Author	Change Summary	Approval Date
v1.0	Executive Privacy Officer	Wording Updates	March 2019
v2.0	Principal Privacy Officer	Wording Updates	29 March 2021

V3.0	Principal Privacy Officer	Review of the PMP and updates to include amendments to the PPIP Act	24 November 2023

Appendix 1: Legislative and Policy Framework

Legislation which icare's PMP is aligned to includes:

- *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIP Act**)
- *Privacy and Personal Information Protection Regulation 2019* (NSW)
- *Health Records and Information Privacy Act 2002* (NSW) (**HRIP Act**)
- *Health Records and Information Privacy Regulation 2022* (NSW)

Exemptions

The IPPs and HPPs in the PPIP Act and HRIP Act do not apply in certain situations or to certain information collected. Different exemptions may apply. Sections 22 – 28 of the PPIP Act and sections 14 – 17A of the HRIP Act detail specific exemptions to the IPPs and HPPs. When considering whether an exemption applies, it is therefore important to determine if the information is simply personal or includes health information.

When considering whether an exemption may apply in a particular situation, the wording of the exemptions contained within the PPIP and HRIP Acts should be consulted, and guidance sought from the Privacy Officer.

Common exemptions include:

- unsolicited information
- personal information collected before 1 July 2000
- health information collected before 1 September 2004
- the individual concerned has consented to the use of their information for a secondary purpose
- law enforcement and investigative purposes
- when it is 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 contemplated
- 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
- finding a missing person
- information sent to other agencies under the administration of the same Minister or Premier for the purposes of informing the Minister or Premier.

Laws authorising non-compliance

Examples of laws which authorise or permit icare agencies to not comply with certain IPPs and HPPs include:

Section 72 of the *Workplace Injury Management and Workers Compensation Act 1998* (NSW)

Insurers are authorised to exchange information held by them in relation to claims

Section 174 of the *Workers Compensation Act 1987* (NSW)

icare may provide information supplied to them by an employer to any insurer for the purpose of assisting the insurer to determine whether the correct premium has been paid under a policy of insurance issued by the insurer.

Section 120 of the *Motor Accidents Compensation Act 1999* (NSW)

icare is authorised to exchange information with SIRA concerning claims under this Act, payments made to or on behalf of participants in the Scheme under the *Motor Accidents (Lifetime Care and Support) Act 2006* (NSW) and the NSW CTP Scheme, and the treatment and care needs of those participants.

icare is authorised to provide to SIRA any information concerning claims under the *Motor Vehicles (Third Party Insurance) Act 1942* (NSW) and the *Transport Accidents Compensation Act 1987* (NSW).

Section 121B of the *Home Building Act 1989* (NSW)

icare may disclose to a person engaged in the administration of this Act information obtained in connection with the exercise of the functions of icare under this Act if the disclosure is for the purpose of assisting in the administration or execution of this Act.

Other Exemptions relevant to icare

The PPIP Act and HRIP Act set out other exemptions of relevance to icare, for example:

Section 27A of the PPIP Act: information exchanges between public sector agencies

icare or its agencies are not required to comply with the IPPs if the agency is providing the information to another public sector agency and the collection, use or disclosure of the information is reasonably necessary for any of the following:

- to allow any of the agencies concerned to deal with, or respond to, correspondence from a Minister or Member of Parliament
- to enable inquiries to be referred between the agencies concerned
- to enable the auditing of the accounts or performance of a public sector agency or group of public sector agencies (or a program administered by an agency or group of agencies).

This exemption does not apply to health information.

Section 27B of PPIP Act: exemptions relating to research

There are special provisions relating to the disclosure of personal information for research purposes. These provisions do not apply to health information.

Generally speaking, icare will always seek consent from the individual to disclose their personal information for research purposes.

In other cases, the information should be de-identified.

The icare Privacy Team should be contacted regarding any proposed use of personal information without consent of the individual for research purposes.

Public Registers/ Memorandums of Understanding

The PPIP and HRIP Acts govern how personal and health information is managed in public registers. icare does not have any public registers that contain personal or health information.

icare does not have any Memorandums of Understanding or referral arrangements with other agencies that would affect how we manage personal or health information.

Other matters affecting how we comply with Privacy Principles

Public Interest Directions

The NSW Privacy Commissioner also issues Public Interest Directions which change the application of some IPPs in certain situations. Public Interest Directions do not override other laws about the handling of information laws which may affect an agency.

NSW Privacy Commissioner has issued the "The Direction under s41(1) of the Privacy and Personal Information Protection Act 1998 in relation to Service NSW and icare's joint payments project" dated 20 September 2023 and which has effect for a period of 12 months. Public Interest Directions are available on the Commissioner's website: https://www.ipc.nsw.gov.au/privacy/nsw-privacy-laws/public-interest-directions

Other Legislation

Other legislation that may also affect the application of the Privacy Principles includes, but is not limited to:

Crimes Act 1900 (NSW)

Under this law, icare must not access or interfere with data in computers or other electronic devices unless we are authorised to do so.

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

Under these law people can apply for access to government information we hold. This information may sometimes include personal or health information. If a person has applied for access to someone else's personal or health information, we must consult with affected third parties. If we decide to release a third party's personal information, we must not disclose the information until the third party has had the opportunity to seek a review of our decision. When accessing government information of another NSW public sector agency in connection with a review, the Information Commissioner must not disclose this information if the agency claims that there is an overriding public interest against disclosure.

Some personal and health information icare agencies hold will not be released under the GIPA Act. Claims information of Workers Insurance are excluded from access applications under the GIPA Act.

For further information on applications to access information under the GIPA Act, please visit our website https://www.icare.nsw.gov.au/access-to-information.

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

Independent Commission Against Corruption Act 1988 (NSW)

Under this law, icare employees must not misuse information obtained in the course of their duties.

Public Interest Disclosures Act 2022 (NSW) (PID Act)

Under the PID Act, a public official, which includes people working within a NSW public sector agency, can make a public interest disclosure (PID) to the Information Commissioner about a failure to properly fulfil functions under the GIPA Act or to the Privacy Commissioner about a non-trivial failure to exercise functions in accordance with the PPIP Act or the HRIP Act.

We note that the definition of personal information under the PPIP Act excludes information about an individual contained in a PID. This means that "personal information" received or collected under the PID Act is not subject to the IPPs or HPPs.

The PID Act requires that we must not disclose information that might identify or tend to identify a person who has made a voluntary PID. This PMP will address how we protect the information we receive in relation to PIDs.

State Records Act 1998 **(NSW) and** ***State Records Regulation 2015*** **(NSW)**

These laws set out the requirements for the creation, management and protection of icare records.