Privacy Management Plan

Insurance and Care NSW (icare)

Workers Compensation Nominal Insurer

NSW Self Insurance Corporation

Dust Diseases Authority

Lifetime Care and Support Authority

Sporting Injuries Compensation Authority

1 Introduction 4
2 About Us 4
2.1 Who we are 4
2.2 What we do 4
2.3 Contacting Us 5
3 Privacy Management Plan Framework 5
3.1 Why we have a privacy management plan 5
3.2 What this Plan Covers 6
3.3 Reviewing the Plan 6
3.4 Legislative and Policy framework 6
3.4.1 Privacy Legislation 6
3.4.2 Relevant Policies and Guidelines 6
4 Staff Responsibilities 6
4.1 Responsibilities of the Privacy Officer 6
4.2 Responsibilities of our staff in general 7
4.3 Agents 7
4.4 Other Suppliers 7
5 What is personal and health information 7
5.1 Personal information 8
5.2 Health information 8
6 Personal information held by icare 8
6.1 Our Stakeholders 8
6.2 Personal and health information held about other individuals 9
6.2.1 Third party consent 11
6.3 External enquiries 11
6.4 Personal and health information held about employees 11
6.5 Website 12
6.5.1 Information collected on the website 12
6.5.2 Cookies 12
6.5.3 Use of the information 12
6.5.4 Exceptions 12
6.5.5 Storage of the information 12
6.5.6 Access to information 13
7 How to access and amend personal information 13
7.1 Informal request 13
7.2 Formal request 13
Why we might not give access to or amend personal or health information 14

7.3 Limits on accessing or amending other people's information 14
8 Review rights and complaints 14
8.1 Internal Review 14
8.1.1 General principles 14
8.1.2 How to apply for internal review 14
8.1.3 What applicants can expect from us 15
8.1.4 Role of the Information and Privacy Commissioner 15
8.2 External Review 15
8.3 Other access requests 16
9 How the Information Privacy Principles Apply 16
9.1 IPPs 16
9.2 HPPs 19
10 Exemptions 19
10.1 Laws authorising non-compliance 20
10.2 Other Exemptions relevant to icare 20
10.3 Public Registers/ Memorandums of Understanding 21
10.4 Other matters affecting how we comply with privacy principles 21
10.4.1 Public Interest Directions 21
10.4.2 Other Legislation 21
11 Promoting the Plan 22
11.1 Executive & Governance 22
11.2 Public awareness 22
12 Forms 23

Version Control

Version	Date	Author(s)
V1	15 Mar 2016	Bethan Lewis

1 Introduction

This plan explains how icare and its agencies, the Workers Compensation Nominal Insurer, the Dust Diseases Authority, the Lifetime Care and Support Authority, the Sporting Injuries Compensation Authority and the NSW Self Insurance Corporation manage personal and health information in line with NSW privacy laws.

2 About Us

2.1 Who we are

On 1 September 2015, Insurance and Care NSW (icare) was established by the *State Insurance and Care Governance Act 2015* to manage the insurance and care schemes in NSW.

icare acts for the Workers Compensation Nominal Insurer and provides services to the Dust Diseases Authority, the Lifetime Care and Support Authority, the Sporting Injuries Compensation Authority and the NSW Self Insurance Corporation. icare reports to the Minister for Finance, Services and Property.

icare was established as part of the 2015 insurance and regulation reforms which abolished the former WorkCover Authority of New South Wales and created three separate entities in its place, the State Insurance Regulatory Authority, SafeWork NSW, and icare. The transition process for these new entities is still ongoing.

Further information about the 2015 reforms is available online at www.insurancereforms.nsw.gov.au.

2.2 What we do

icare provides services including staff, facilities, and investment strategies and direction for the following entities:

Workers Compensation Nominal Insurer

The Workers Compensation Nominal Insurer (**Workers Insurance**) was established by the *Workers Compensation Act 1987.* Workers Insurance provides workers compensation insurance to approximately 70 per cent of the NSW workforce.

Workers Insurance has agreements with five other insurers (CGU, Allianz, GIO, QBE and Employers Mutual) which manage claims for injured workers and provide policies to employers on its behalf.

Dust Diseases Authority

The Dust Diseases Authority (**Dust Diseases Care**) was established by the *Workers' Compensation (Dust Diseases) Act 1942.* It provides compensation payments and arranges healthcare for people with a work related dust disease.

Dust Diseases Care can also make grants for the purpose of clinical or research work and for the purpose of providing assistance to groups or organisations that provide support for victims of dust diseases or their families.

Lifetime Care and Support Authority

The Lifetime Care and Support Authority (**Lifetime Care**) was established by the *Motor Accidents*

(Lifetime Care and Support) Act 2006. Lifetime Care provides treatment, rehabilitation and care for people severely injured in motor accidents in NSW, regardless of who was at fault in the accident.

Sporting Injuries Compensation Authority

The Sporting Injuries Compensation Authority was established by the *Sporting Injuries Insurance Act 1978*. The Sporting Injuries Compensation Authority provides compensation for certain injuries resulting from sporting or athletic activities.

The Sporting Injuries Compensation Authority also compiles statistics regarding the incidence of injuries from sporting or athletic activities and works with other bodies on policies to reduce the incidence of injuries resulting from sporting or athletic activities.

NSW Self Insurance Corporation

The NSW Self Insurance Corporation (Self Insurance) was established by the *NSW Self Insurance Corporation Act 2004.* Self Insurance administers a number of managed fund schemes serving NSW Government agencies and their current and former employees. The Government's self-insurance scheme, known as the Treasury Managed Fund (TMF), is the largest. The TMF provides protection for all asset and liability exposures, except Compulsory Third Party (CTP) motor vehicle insurance, for most general Government agencies. The TMF provides cover for workers compensation, public liability, property, motor vehicle and miscellaneous insurance.

Additionally, Self Insurance administers several closed Government schemes. These include the Governmental Workers Compensation Account, Transport Accidents Compensation Fund, Pre-Managed Fund Reserve and Rail Scheme.

Self Insurance also underwrites home warranty insurance and manages the Home Building Compensation Fund (**HBCF**).

2.3 Contacting Us

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

Web: www.icare.nsw.gov.au

Email: privacy@icare.nsw.gov.au

Phone: (02) 4321 5000

Mail: icare Privacy Officer, Locked Bag 2906 Lisarow NSW 2250

Visit: Head office is located at 321 Kent Street, Sydney NSW 2000

3 Privacy Management Plan Framework

3.1 Why we have a privacy management plan

Given the nature of our work, we collect, use, hold and disclose the personal and/or health information of many people. We take seriously our responsibility to look after personal and health information and are bound by law in the way we collect, use, store and disclose it. icare has a privacy management plan to show stakeholders and employees how we manage personal information in line with the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**) and health information in line with the *Health Records and Information Privacy Act 2002* (**HRIP Act**)

We are also required by law to have such a plan, under section 33 of the PPIP Act.

3.2 What this Plan Covers

Our plan includes information about:

- icare policies and practice to ensure compliance by the agency with the PPIP Act and or HRIP Act
- our internal review procedures for handling privacy complaints.
- how we educate our staff about those policies and practices within icare

3.3 Reviewing the Plan

Our plan will be reviewed in November 2016. Thereafter it will be reviewed at a minimum every two years, but more frequently when legislative, administrative or systemic changes occur that affect the way we manage the personal and health information we hold.

3.4 Legislative and Policy framework

3.4.1 Privacy Legislation

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

Privacy and Personal Information Protection Amendment (Exemptions Consolidation) Act 2015

Privacy and Personal Information Protection Regulation 2014

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

Health Records and Information Privacy Regulation 2012

3.4.2 Relevant Policies and Guidelines

Below is a list of key privacy-related policies which apply to icare:

- Code of Conduct and Ethics Policy
- External Data Release Policy
- Records Management Policy
- Customer Service Charter
- Workplace Issues Grievance
- Recordkeeping Governance Policy
- Acceptable usage of electronic communication devices and services policy
- NSW Government Information Classification and Labelling Guidelines
- Information Security Policy
- Managing ICT Access Policy
- Transitional Information Handling Policy
- Information Classification and Handling Policy
- Mobile Phone Policy
- Facilities & Assets Security Policy

These policies are currently under review. If you have any queries regarding what policies or guidelines apply to icare, please contact the Privacy Officer.

4 Staff Responsibilities

4.1 Responsibilities of the Privacy Officer

icare's Privacy Officer is responsible for the ongoing training and education of icare staff members (including any third party service providers or consultants) about their obligations under the PPIP Act and HRIP Act, by:

- ensuring this plan remains up to date

- making a copy of this plan available to all current and incoming staff, and contractors
- informing staff and contractors of any changes to the plan
- ensuring relevant privacy documents are consolidated and made available through the icare intranet pages
- conducting or arranging staff training sessions on privacy matters as required
- being available to answer any questions staff or contractors may have about their privacy obligations, and
- ensuring the organisation meets its annual report obligations.

To meet our annual reporting obligations each year, our annual report includes a statement of the action undertaken by the agencies to ensure they comply with the requirements of the PPIP Act and provide statistical details of any review conducted by or on behalf of the agencies under the PPIP Act.

The icare Privacy Officer can be contacted as follows:

Email: privacy@icare.nsw.gov.au

Phone: (02) 4321 5000

Mail: Privacy Officer Locked Bag 2906 Lisarow NSW 2250

Visit: Head office is located at 321 Kent Street, Sydney NSW 2000

4.2 Responsibilities of our staff in general

All staff and contractors of icare or its agencies must comply with the PPIP Act and HRIP Act. Both Acts contain criminal offence provisions applicable to staff and contractors who use or disclose personal information or health information without authority. This plan is intended to assist staff to understand and comply with their obligations under those Acts. If staff members are uncertain as to whether certain conduct may breach their privacy obligations, they should seek the advice of the Privacy Officer.

WARNING

It is a criminal offence, punishable by up to two years' imprisonment, an $11,000 fine (or both), for any person employed or engaged by icare (including former employees and contractors) to intentionally use or disclose any personal information or health information about another person, to which the employee or contractor has or had access in the exercise of his or her official functions, except in connection with the lawful exercise of his or her official functions.

4.3 Agents

In some cases icare agencies employ agents, such as other insurance companies to act on their behalf to provide services. Those agents are also bound by the PPIP Act and HRIP Act.

4.4 Other Suppliers

icare often engages private companies to provide services to the organisation. Those suppliers are required to comply with the PPIP Act and HRIP Act for the purposes of the services provided to icare or its agencies.

5 What is personal and health information

We collect and receive many different kinds of personal and health information in order to conduct our work. Due to the nature of our work, we may collect this information in large volumes. Definitions of personal and health information are provided below.

5.1 Personal information

Personal information is defined in s4 of the PPIP Act. Essentially, personal information is information or an opinion that identifies, or could reasonably identify, an individual.

Examples of personal information include 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.

A person's identity may be apparent where neither the name nor a photograph is involved, but the information about the person is such that it could not be referring to anyone else.

Section 4(3) excludes certain types of information from the definition. 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

• A number of exceptions relating to law enforcement investigations.

Some examples of information which is NOT personal information include recruitment records and referee reports, as well as information that is published or available on the internet. The PPIP Act also excludes certain information that may be held in connection with some activities authorised under different legislation.

For detailed information about information excluded from the definition of personal information, consult sections 4(3) and 4A of the PPIP Act or contact the Privacy Officer.

5.2 Health information

Health information is a highly sensitive type of information which must be handled with a great deal of care and respect. Health information is defined in section 6 of the HRIP Act and includes:

- information or an opinion about the physical or mental health or a disability (at any time) of an individual, or an individual's express wishes about the future provision of health services to him or her, or a health service provided, or to be provided, to an individual
- other personal information collected to provide, or in providing, a health service
- other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances
- other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of a genetic relative of the individual, or
- healthcare identifiers.

The definition of health information does not include health information excluded by the HRIP Act. This might be a piece of health information, a class of health information or health information contained in a class of documents.

6 Personal information held by icare

6.1 Our Stakeholders

We may collect personal or health information from, or disclose personal or health information to, our stakeholders to do our work. These stakeholders include:

- workers
- care scheme participants
- insurers
- government regulators
- other state and federal government agencies and authorities (including Ministers offices and state owned corporations)
- courts and tribunals
- Parliament
- private sector companies
- academics and researchers
- medical and allied health professionals
- non-government organisations
- solicitors and other legal representatives
- unions

6.2 Personal and health information held about other individuals

Given the diversity of functions across icare, the range of personal information held is extensive and wide ranging.

The personal and health information collected by and provided to icare and its agencies may be received in the form of email, in writing, over the phone, by fax, in person, online, in an application or claim form, from surveillance, photographs and various forms of electronic storage or recording devices.

In some circumstances the provision of personal information is voluntary, in others compulsory.

Below is a brief outline of the functions of the icare agencies and the main types of personal and health information collected:

Agency	Functions	Types of information held
Workers Insurance	provision of workers compensation insurance: • management of scheme agents; and • direct claims management of uninsured liabilities (see also *Workers Compensation Act 1987)* • management of Sporting Injuries compensation scheme (see also *Sporting Injuries Insurance Act 1978)*	• names, contact details, dates of birth, employment, wages, voice recordings, photos, video, complaints, banking details • physical and mental health records, medical certificates, medical reports, disability, fatality, medical and allied health care/services provision, future health care wishes, details of injurious incidents, witness statements; and • information given as part of applications, for example for government held information sought under freedom of information laws and workers compensation premium appeals.
Dust Diseases Care	• provision of compensation, medical care and services for workers and families affected by work related dust diseases (see also *Workers' Compensation (Dust Diseases) Act 1942*	• names, contact details, dates of birth, employment, wages, family members and associates, banking details, photos, video; and • physical and mental health records, medical certificates, medical reports, disability, fatality, medical and allied health care/services provision, future health care wishes
Lifetime Care	• provision of compensation, medical care and services for people severely injured in motor accidents in NSW (see also *Motor Accidents (Lifetime Care and Support) Act 2006)*	• names, contact details, dates of birth, employment, wages, family members and associates, voice recordings, photos, video, complaints, banking details; and • physical and mental health records, medical certificates, medical reports, disability, fatality, medical and allied health care/services provision, future health care wishes, details of injurious incidents, witness statements
Self Insurance	• provision of insurance for government agencies • representing the interests of	• names, contact details, dates of birth, employment, wages, family members and associates, voice recordings, photos, video,

	NSW Government on all insurance matters • management of HBCF (see also 'About us' section and *NSW Self Insurance Corporation Act (2004)*).	complaints, banking details • physical and mental health records, medical certificates, medical reports, disability, fatality, medical and allied health care/services provision, future health care wishes, details of injurious incidents, witness statements; and • information given as part of applications, for example for government held information sought under freedom of information laws and workers compensation premium appeals.

Wherever possible, information is collected directly from the individual. Collection of information about a third party is kept to a minimum and only occurs when it is unreasonable or impractical to collect it from the individual, or where the law otherwise permits or requires us to do so.

6.2.1 Third party consent

As noted previously, if a person lacks the capacity to provide or seek information yourself, they may nominate a contact person. A copy of the privacy consent form that will need to be completed and provided is in the '**Forms'** section.

6.3 External enquiries

If someone writes to icare agencies, we keep a full copy of their correspondence. Our phones display the number of the person calling (except for private numbers). The individual phones store the numbers for the last 10 calls received, and our telephone system keeps a record of all numbers that have called icare. They are retained as a record and not used.

Telephone calls made to the 131050 call centre are recorded electronically for quality and training purposes. They are periodically deleted.

6.4 Personal and health information held about employees

For various reasons, such as leave management, workplace health and safety and operational requirements, icare keeps staff records including:

- Documents related to the recruitment process
- Payroll, attendance and leave records
- Banking details and tax file numbers
- Training records
- Workers compensation records
- Workplace health and safety records
- Records of gender, ethnicity and disability of employees for equal opportunity
- reporting purposes
- Medical conditions and illnesses
- Next of kin
- Secondary employment
- Conflicts of interests.

- Photos and/or video

This information is collected directly from employees and will be managed in accordance with the provisions of the PPIP and HRIP Acts.

6.5 Website

icare manages the website www.icare.nsw.gov.au.

6.5.1 Information collected on the website

icare automatically records information that identifies, for each page accessed:

- the IP (Internet Protocol) address of the machine which has accessed it;
- the top-level domain name (for example .com, .gov, .au, .uk etc.);
- the address of the server;
- the date and time of the visit to the site; and
- the pages accessed and documents downloaded.

6.5.2 Cookies

'Cookies' are small pieces of text data that a web server can store on, and later retrieve from, a user's computer. The icare site does not use cookies.

6.5.3 Use of the information

The information collected during each visit is aggregated with similar logged information and published in reports in order for icare to identify patterns of usage of the site. This information assists icare in improving the site and the services offered on it.

icare does not disclose or publish information that identifies individual computers, without consent or otherwise in accordance with the PPIP Act.

6.5.4 Exceptions

icare will collect, use and disclose more extensive information than stated above in the following circumstances:

- unauthorised attempts to access files which are not published icare pages;
- unauthorised tampering or interference with files published on the site;
- unauthorised attempts to index the contents of the site by other sites;
- attempts to intercept messages of other users of the site;
- communications which are defamatory, abusive, vilify individuals or groups or which give rise to a suspicion that an offence is being committed; and
- attempts to otherwise compromise the security of the web server or breach the laws of the State of New South Wales or Commonwealth of Australia

icare reserves the right to make disclosures to relevant authorities where the use of the icare site raises a suspicion that an offence is being, or has been, committed.

In the event of an investigation, icare will provide access to data to any law enforcement agency that may execute a warrant to inspect icare's logs.

6.5.5 Storage of the information

The information collected is stored in an appropriately secure format and held by icare for archival purposes. icare retains the information for at least one year. When the information is no longer required for the purposes for which it was collected it is deleted.

icare captures this information on its own computers and through the use of third-party analytical software such as Google Analytics. Access to the raw data is restricted to a limited number of officers in icare for the purpose of analysis and to report on the success of the site in meeting icare's communication and access objectives.

7 How to access and amend personal information

In the majority of cases, employees and members of the public have the right to access the personal and health information we hold about them.

In the majority of cases, people also have the right to amend their personal or health information we hold, for example, if they need to update their contact details.

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

7.1 Informal request

Informal requests do not need to be in writing.

People can request access to or amendment of their personal or health information by contacting the Privacy Officer by telephone on (02) 4321 5000 or by email at privacy@icare.nsw.gov.au

People can request access to your own employee records by contacting People Engagement by emailing people@icare.nsw.gov.au.

People will need to verify their identity and in some circumstances, particularly if it is sensitive information, we may ask you to make a formal application.

We aim to respond to informal requests within 5 working days. We will tell applicants how long the request is likely to take, particularly if it may take longer than first expected. We will contact them to advise the outcome of the request. If they are unhappy with the outcome of an informal request, they can make a formal application to us.

7.2 Formal request

Formal requests need to be made in writing.

People do not need to ask informally before making a formal application, and they can make a formal application if they have already asked informally.

A formal application can be made to icare by email, fax or post (contact details are provided above in the '**Contacting Us**' section). The application should:

- include your name and contact details
- state whether you are making the application under the PPIP Act (personal information) or HRIP Act (health information)
- explain what personal or health information you would like to access or amend, and
- explain how you would like to access or amend it.

We aim to respond in writing to formal applications within 20 working days. We will contact applicants to advise how long the request is likely to take, particularly if it may take longer than expected.

If applicants think we are taking an unreasonable amount of time to respond to an application, they have the right to seek an internal review. Before seeking an internal review, we encourage applicants to contact our office to ask for an update or timeframe for response.

If applicants disagree with the outcome of the application, they have the right to seek an internal review.

Why we might not give access to or amend personal or health information
If we decide not to give a person access to or amend their personal or health information, we will clearly explain our reasons. For example, the *Government Information (Public Access) Act 2009* (GIPA Act) excludes a person from applying for information contained within Workers Insurance and Dust Diseases care claim files and so may not be subject to release. Further information about the relationship between privacy and the GIPA Act is available under the '**Other access requests'** section below.

7.3 Limits on accessing or amending other people's information

We are usually restricted from granting access to someone else's personal and health information. While the PPIP Act and the HRIP Act give a person the right to access their own information, the Acts generally do not give a person the right to access someone else's information.

However, under s26 of the PPIP Act, a person can give us consent to disclose their personal information to someone that would not normally have access to it. Also, under s7 and s8 of the HRIP Act, an "authorised person" can act on behalf of someone else. The health protection principles also contain information about other reasons we may be authorised to disclose health information, such as in the event of a serious and imminent threat to the life, health and safety of an individual, to find a missing person or for compassionate reasons. If none of these scenarios is relevant, a third party could also consider making an application for access to government information under the GIPA Act (further information on the GIPA Act is available below in the '**Other access requests'** section).

It is quite common for consent to be granted by an individual when they are young and would like their parents to act on their behalf, when contact worsens anxiety conditions or when an individual is mentally or physically unfit to represent themself.

When a person requires someone else to act on their behalf, a Privacy Consent Form needs to be completed. A copy of the form is available in the '**Forms**' section below.

8 Review rights and complaints

8.1 Internal Review

8.1.1 General principles

If a person considers that icare or its agencies has breached the PPIP Act or HRIP Act in relation to their personal or health information, or doesn't agree with the outcome or progress of their application to access or amend their personal or health information, they have the right to seek an internal review.

The following general principles are relevant to applications for internal review:

- Privacy Complaints can be made either directly to the NSW Privacy Commissioner or by applying to icare for an 'internal review' of the conduct a person believes breaches an Information Privacy Principle and/or a Health Privacy Principle.
- Complaints to the NSW Privacy Commissioner can only result in a conciliated outcome, rather than a binding determination.
- A person cannot seek an internal review for a breach of someone else's privacy, unless they are an authorised representative of the other person.
- An application for an internal review must be made within six months from when a person first becomes aware of the breach, although icare may also consider a late application for internal review.

8.1.2 How to apply for internal review

To apply for an internal review, icare has an application form in the '**Forms**' section below. Although we encourage use of the form, it is not compulsory. Any other relevant material may be submitted along with the application.

Requests for internal review should be sent to the icare Privacy Officer by email, fax or post (details above in '**Contacting Us'** section) and needs to:

- be in writing

- be addressed to icare, and
- include a return address in Australia

Applications in other languages will be accepted and translated, and all acknowledgments and correspondence from icare will be translated into the applicant's preferred language. If the applicant is not literate in English and/or their first language and there is no organisation making the application on their behalf, the Privacy Officer will help write the application, using a professional interpreter if necessary.

8.1.3 What applicants can expect from us

- The application will be acknowledged within 5 working days and will include an expected completion date
- We will inform the NSW Privacy Commissioner of the application and will provide them with a copy of the written complaint. The NSW Privacy Commissioner is entitled to make submissions and provide relevant material if necessary
- Either the icare Privacy Officer, or another person not involved in the conduct which is the subject of the complaint, who is an employee or an officer of the agency and is qualified to deal with the subject matter of the complaint, will conduct the review
- The internal review will be completed within 60 days of receiving the application
- We will follow the NSW Privacy Commissioner's Internal Review Checklist (available at ipc.nsw.gov.au) and give consideration given to any relevant material submitted by the applicant and/or the NSW Privacy Commissioner
- In making a decision, we may decide to:
  - 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, and/or
  - implement administrative measures to ensure that the conduct will not occur again.
- The applicant will be informed of the outcome within 14 days of the internal review being decided, including:
  - the findings of the review
  - the reasons for those findings
  - the action icare proposes 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 (NCAT).

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

8.1.4 Role of the Information and 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 the application for internal review.

In reviewing the application, icare will continue to keep the Privacy Commissioner informed of the progress of the internal review, the findings of the review and the proposed action to be taken by icare in relation to the internal review. Any submissions made by the Privacy Commissioner to the agency will be taken into consideration when making our decision.

8.2 External Review

If an applicant is unhappy with the outcome of the internal review, they can apply to NCAT to review the decision. If icare has not completed the internal review within 60 days, they can also take the matter to NCAT.

To seek an external review, application must be made to NCAT. Generally a person has 28 days from the date of the internal review decision to seek an external review. An internal review by icare must be requested before a person has the right to seek an external review.

NCAT has the power to make binding decisions on an external review, including ordering icare to pay damages. For more information about seeking an external review including current forms and fees, please contact NCAT:

Website: www.ncat.nsw.gov.au

Phone: (02) 9377 5711

Visit/post: NSW Civil & Administrative Tribunal, Administrative and Equal Opportunity Division, Level 10, John Maddison Tower, 86-90 Goulburn Street, Sydney NSW 2000.

8.3 Other access requests

icare and its agencies are all subject to the *Government Information (Public Access) Act 2009* (GIPA Act). Under this law anyone can apply for access to government information we hold. Sometimes this information may 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.

Some personal and health information icare agencies hold will not be released under the GIPA Act. Claims information of Dust Diseases Care and 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 www.icare.nsw.gov.au.

9 How the Information Privacy Principles Apply

The PPIP Act sets out 12 Information Protection Principles (IPPs). icare must follow these principles for collecting, storing, using and disclosing personal information. The HRIP Act sets out 15 Health Privacy Principles (HPPs) in relation to health information.

This section sets out icare's approach to these principles. Specific applications of these principles should be built into icare policies and procedures relating to collection, storage, use or disclosure of personal or health information.

There are a number of exemptions to these IPPs and HPPs, which are discussed below in the '**Exemptions**' Section

9.1 IPPs

COLLECTION

1. Lawful

icare agencies will only collect personal information for a lawful purpose, which is directly related to our functions or activities and necessary for that purpose.

2 Direct

icare will only collect personal information directly from the person concerned where possible, unless they have authorised collection from someone else or the person is under the age of 16 and the information has been provided by a parent or guardian.

In some instances we collect information about third parties. Collection of information about a third party is kept to a minimum and only occurs when it is unreasonable or impractical to collect it from the individual, or where the law otherwise permits or requires us to do so.

3 Open

icare agencies inform people why their personal information is being collected, what it will be used for, and to whom it will be disclosed. We tell people how they can access and amend their personal information and the consequences if they decide not to give their personal information to us.

4 Relevant

icare agencies ensure that personal information is relevant, accurate, is not excessive and does not unreasonably intrude into the personal affairs of people.

In developing each of the services we provide, a decision is made about the level of personal information appropriate to be collected to enable sound decision making and ensure we can maintain accurate records, but without requesting unnecessary information.

STORAGE

5 Secure

icare agencies store personal information securely, keep it no longer than necessary and destroy it appropriately. We protect personal information from unauthorised access, use or disclosure

Systems and information management

icare's information security posture is to be consistent with the NSW Government's *Digital Information Security Policy*. Accordingly, icare have adopted the NSW Government's *Classification, Labelling and Handling Guidelines* and established an Information Security Management System (ISMS) compliant with ISO 27001. We are building IT Governance mechanisms and our new systems are being designed with "Data must be appropriately secured" as a principle. Whilst the ISMS is operating today, our intent is to have it certified against ISO 27001 by 30 June 2017.

Physical security

Our hard copy information is mainly located in our office locations. We archive older physical files in a secure storage facility in compliance with the *State Records Act 1998*. Our staff members have key card access to our office. Our offices are locked outside of business hours.

We keep physical files securely stored when we are not using them. We do not leave sensitive information on the printer and use secure printing where appropriate. We use locked bins for sensitive documents that need to be destroyed.

ACCESS AND ACCURACY

6 Transparent

icare agencies are transparent about the personal information we store about people, why we use the information and about the right to access and amend it.

When we collect information in the exercise of an administrative or educative function, we will take reasonable steps to ensure that, before the information is collected, or as soon as practicable after collection, an individual is made aware of the purpose for collection, the intended recipients of the information, details of the agency that collects or holds the information, whether the supply of information by an individual is required by law or is voluntary, and any consequences for the individual if the information is not provided.

7 Accessible

icare allows people to access their own personal information without unreasonable delay or expense (see also '**How to access or amend personal information**')

8 Correct

icare allows people to update, correct or amend their personal information where necessary.

We ensure the accuracy of the information by collecting it directly from the individual wherever possible and checking it with the individual before using it. As we collect the information of such a large number of people, we attempt to collect information such as date of birth and middle name so that we can differentiate individuals.

Where information about an individual is collected from a third party we use additional identifiers such as middle name and date of birth to ensure we are receiving the information of the correct individual.

Inaccurate information is required to be updated where necessary and where it is possible to do so. In some cases, evidence of the required change may be requested, for example, to apply name changes or changes to date of birth. In line with the privacy and health protection principles, action taken to ensure information is accurate before it is used will depend on the information in question. Where practical, multiple separate sources of the same information will be limited in favour of having one authoritative source that can be maintained.

Individuals can correct information held about themselves or request information be corrected through the accessing information processes. See the above 'How to access and amend personal information' section of this plan for further information on how to do this (see also '**How to access or amend personal information**')

USE

9 Accurate

icare agencies make sure that personal information is relevant, accurate and up to date before using it.

10 Limited

icare agencies only use personal information for the purpose we collected it for, unless the person consents to us using it for an unrelated purpose.

Personal and health information is not transmitted across the organisation but is limited to those people within the organisation who need it to exercise their functions.

DISCLOSURE

11 Restricted

icare agencies only disclose personal information with a person's consent, unless they were already informed that the information would be disclosed, or the person has been made aware that information of that kind is usually disclosed, or if disclosure is necessary to prevent a serious and imminent threat to any persons health and safety

12 Safeguarded

icare agencies will take particular care not to disclose sensitive personal information without a person's consent. For example, information about ethnic or racial origin, political opinions, religious or philosophical beliefs, sexual activities or trade union membership. We will only disclose sensitive information without consent in order to deal with a serious or imminent threat to any person's health and safety.

9.2 HPPs

The first 11 HPPs are the same the IPPS. In addition to the above principles, the following principles apply to the collection, storage, use and disclosure of health information:

IDENTIFIERS AND ANONYMITY

12 Not identified

icare does not use unique identifiers for health information, as we do not need them to carry out our functions efficiently.

13 Anonymous

People have the option of receiving services from icare anonymously, where this is lawful and practicable. In practice, given the nature of the services we provide, this would rarely by practicable.

TRANSFERRALS AND LINKAGE

14 Controlled

We do not usually transfer health information outside of NSW. When we do, it is in order to provide necessary services to individuals. icare takes reasonable steps to ensure that the information that it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Health Privacy Principles.

15 Linkage of Health Records

We do not currently use a health records linkage system.

10 Exemptions

The Information and Health Privacy Principles in the PPIP Act and HRIP Act do not apply in certain situations or to certain information collected. Different exemptions may apply between an IPP and its equivalent HPP. 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 to a particular situation, the wording of the exemptions contained within PPIP Act should be consulted, and guidance sought from the Privacy Officer. Sections 22 – 28 of the PPIP Act and sections 14 – 17A of the HRIP Act detail specific exemptions to the IPPs and HPPs.

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 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, and

- information sent to other agencies under the administration of the same Minister or Premier for the purposes of informing the Minister or Premier.

10.1 Laws authorising non-compliance

Examples of laws which authorise or permit icare agencies to not comply with certain Information and Health Privacy Principles include:

Section 72 of the *Workplace Injury Management and Workers Compensation Act 1998*:

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

Sections 243 and 243A of the *Workplace Injury Management and Workers Compensation Act 1998*

Workers Insurance may disclose any information obtained in connection with the administration or execution of this Act to SafeWork NSW, and the Chief Commissioner of State Revenue under the *Taxation Administration Act 1996*, and the Insurance and Superannuation Commissioner under the *Insurance and Superannuation Commissioner Act 1987* of the Commonwealth.

Section 174 of the *Workers Compensation Act 1987*

Workers Insurance 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*

Lifetime Care 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* and the treatment and care needs of those participants.

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

Section 121B of the *Home Building Act 1989*

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

10.2 Other Exemptions relevant to icare

The *Privacy and Personal Information Protection Amendment (Exemptions Consolidation) Act 2015* sets out other exemptions of relevance to icare:

Section 27A 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:

(i) to allow any of the agencies concerned to deal with, or respond to, correspondence from a Minister or member of Parliament, or

(ii) to enable inquiries to be referred between the agencies concerned, or

(iii) 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 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 Privacy Officer should be contacted regarding any proposed use of personal information without consent of the individual for research purposes.

10.3 Public Registers/ Memorandums of Understanding

The PPIP/ 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.

10.4 Other matters affecting how we comply with privacy principles

10.4.1 Public Interest Directions

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

There are no public interest directions relevant to icare at present

10.4.2 Other Legislation

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

Crimes Act 1900

Under this law we 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 (GIPA Act) and *Government Information (Public Access) Regulation 2009*

Under this law people can apply for access to government information we hold. Sometimes this information may 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.

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.

Independent Commission Against Corruption Act 1988

Under this law we must not misuse information we have obtained in the course of doing our jobs.

Public Interest Disclosures Act 1994 (PID Act)

Under the PID Act 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.

We note that the definition of personal information under the PPIP Act excludes information 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 PID. This plan will address how we protect the information we receive in relation to PIDs.

State Records Act 1998 and State Records Regulation 2010

This law sets out when we can destroy our records. It also authorises the State Records Authority to establish policies, standards and codes to ensure that NSW public sector agencies manage their records appropriately.

11 Promoting the Plan

11.1 Executive & Governance

icare is committed to transparency about how we comply with the PPIP Act and HRIP Act, which is reinforced by:

- endorsing the plan and making it publicly available
- reporting on privacy in our annual reports in line with the *Annual Reports (Statutory Bodies) Act 1984*
- identifying privacy issues when implementing new systems
- using the plan as part of induction for new staff, contractors etc, and
- undertaking a periodic privacy governance and compliance review.

In addition, we make sure our staff are aware of and understand this plan, particularly how it applies to the work they do, by:

- writing this plan in a practical way so our staff can understand what their privacy obligations are, how to manage personal and health information in their work and what to do if unsure about their privacy obligations
- publishing the plan in a prominent place on our intranet
- highlighting the plan at least once a year (for example, during Privacy Awareness Week).

11.2 Public awareness

This plan is a commitment of service to our stakeholders of how we manage personal information and health information. As it is central to how we do business, this plan is easy to access and easy to understand for people from all kinds of backgrounds.

Additionally, we are required to make this plan publicly available as open access information under the GIPA Act.

We aim to promote public awareness of this plan by:

- writing the plan in plain English
- publishing the plan in a prominent place on our website
- providing hard copies of the plan free of charge on request
- telling people about the plan when we answer questions about how we manage personal information and health information.

12 Forms

1. Privacy Consent Form
2. Internal Review Form

Privacy Consent Form

Privacy and Personal Information Protection Act 1989 (NSW) / Health Records and Information Privacy Act 2002 (NSW)

icare Privacy Officer, phone: (02) 4321 5526 email: privacy@icare.nsw.gov.au

WHEN TO USE THIS FORM: This form should be used to provide express consent from an individual to icare to interact with a nominated third party in relation to collection, use or disclosure of the individual's personal or health information.

THIRD PARTY PROOF OF IDENTITY: If the information is collected in person, the authorised third party will need to prove their identity before information will be provided. Identity can be proved by provision of a current Australian driver's license, a Proof of Age Card, a current Australian passport.

HOW PERSONAL INFORMATION COLLECTED ON THIS FORM WILL BE USED: The personal information on this form will be used to verify the identity of the individuals concerned, contact the individuals to clarify any aspects of this consent and manage the liaison between the individuals and icare.

HOW TO LODGE YOUR THIRD PARTY AUTHORITY FORM: Send your completed form and any supporting documents to: privacy@icare.nsw.gov.au or via mail to: icare Privacy Officer, Locked Bag 2906 Lisarow NSW 2250.

For information about privacy and protection of personal information, visit our website at www.icare.nsw.gov.au .

1. Individual's Details

Surname: ..... **Title**: Mr / Ms

Other names: .....

Postal address: ..... **Postcode**: .....

Daytime telephone: ..... **Facsimile**:.....

Email: .....

Proof of Identity

Note: to protect privacy, this consent will not be accepted as third party authorisation without proof of your identity

Please attach a certified copy of one of the following documents:

- ☐ current Australian driver's licence or Proof of Age card, or
- ☐ current Australian passport, or
- ☐ other proof of signature and current address details

2. Third Party's Details

Surname: ..... **Title**: Mr / Ms

Other names: .....

Postal address: ..... **Postcode**: .....

Daytime telephone: ..... **Facsimile**:.....

Email: .....

3. Applicant's express consent

I, *[enter full name of individual]*

_____,

authorise *[enter full name of third party]*

_____

to act on my behalf in relation to the following matter/s *[specify the purpose of this consent]*

_____

_____. This consent will remain in force until it is rescinded or amended by the applicant, or until *[specify date]:* _____.

Applicant's signature: .....

Date: .....

Authorised third party's signature: .....

Date: .....

Office use only

Date application received:.....

File reference:

General information about the PPIP Act and HRIP Act is available by calling the Information and Privacy Commission NSW (IPC) on 1800 472 679 or visit the IPC's website: www.ipc.nsw.gov.au

icare™

Privacy complaint: Internal review application form

How to use this form

This is an application[1] for review of conduct under: (please select one)

- s53 of the **Privacy and Personal Information Protection Act 1998** (PPIP Act) ☐
- s21 of the **Health Records and Information Privacy Act 2002** (HRIP Act) ☐

1	Name and address of the agency[2] you are complaining about:
2	Your full name:
3	Your postal address: Telephone number: Email address:
4	If the complaint is on behalf of someone else, please provide their details (*name and contact details*): What is your relationship to this person (eg. parent)? Is the person capable of making the complaint by himself or herself? ☐ yes ☐ no (If yes please provide documentation as to why they cannot make the application by themselves)
5	What is the specific conduct[3] you are complaining about? *(see footnote for explanation of "conduct")* *(if there is not enough room attach supporting documentation)*
6	Please tick which of the following describes your complaint: *(you may tick more than one option)* ☐ collection of my personal or health information ☐ security or storage of my personal or health information ☐ refusal to let me access or find out about my own personal or health information ☐ accuracy of my personal or health information ☐ use of my personal or health information ☐ disclosure of my personal or health information ☐ other ☐ unsure
7	When did the conduct occur (date)? *(please be as specific as you can)*

[1] It is not a requirement under the PPIP Act or the HRIP Act that you complete an application form. This form is designed for your convenience only. However, you must make a written request is some form to the agency for the matter to be a valid internal review.

8	When did you first become aware of this conduct (date)?
9	You need to lodge this application within six months of the date at Q.8. If more than six months has passed, you will need to ask the agency for special permission to lodge a late application. Please explain why you have taken more than six months to make your complaint *(for example: I had other urgent priorities – list them, or while the conduct occurred more than six months ago, I only recently became aware of my privacy rights, etc)*: *(if there is not enough room attach supporting documentation)*
10	What effect did the conduct have on you?
11	What effect might the conduct have on you in the future?
12	What would you like to see the agency do about the conduct? *(for example: an apology, a change in policies or practices, your expenses paid, damages paid to you, training for staff, etc.)*

I understand that this form will be used by the agency to process my request for an internal review. I understand that details of my application will be referred to the Privacy Commissioner in accordance with: section 54(1) of the *Privacy and Personal Information Protection Act*; or section 21 of the *Health Records and Information Privacy Act*; and that the Privacy Commissioner will be kept advised of the progress of the internal review.

Your signature: _____

Date:

SEND THIS FORM TO **icare** via email privacy@icare.nsw.gov.au or post: Privacy Officer, icare, GPO Box 4052, Sydney NSW 2001

Keep a copy for your records.

For more information on the PPIP Act or the HRIP Act visit our website: www.ipc.nsw.gov.au

2 The PPIP Act regulates NSW state government departments, area health services, most other state government bodies, and NSW local councils. Each of these is defined as a "public sector agency". The HRIP Act regulates private and public sector agencies and private sector persons.

3 "Conduct" can include an action, a decision, or even inaction by the agency. For example the "conduct" in your case might be a *decision* to refuse you access to your personal information, or the *action* of disclosing your personal information to another person, or the *inaction* of a failure to protect your personal information from being inappropriately accessed by someone else.