icare™
Insurance and Care NSW

Privacy and Data Breach Policy

v2.0 November 2024

Contents

1. Purpose

This Privacy and Data Breach Policy (policy):

- Explains how icare collects and manages personal and health information, which it needs to collect for the purposes of exercising its functions and providing services; and
- Serves as icare's Data Breach Policy and sets out how icare will respond to a Data Breach (defined in section 3.4 below), the roles and responsibilities of people working at icare in relation to managing a Data Breach and the steps icare will follow if a breach occurs.

icare needs to collect, access, use and disclose personal or health information as part of its usual business operations and to effectively and efficiently provide services.

icare is committed to protecting the privacy of all individuals whose personal or health information it collects and handles. This policy sets out the key principles and commitment to action for icare to:

- Achieve the goal of ensuring icare responsibly handles and protects all personal information that it collects and possesses;
- Comply with icare's legal and regulatory obligations as a public sector agency under the Privacy and Personal Information Protection Act 1998 (the PPIPA) and the Health Records and Information Privacy Act 2002 (the HRIPA) and the icare values; and
- Appropriately respond and deal with Data Breaches.

This supports icare's purpose that we care for the people of NSW, building confidence and trust so our communities can thrive. Further information on icare's purpose and values is available on icare's website at: https://www.icare.nsw.gov.au/about-us/our-strategy.

This policy is supplemented by the icare Privacy Management Plan (**PMP**) which provides further detailed information on how icare collects, uses, discloses and disposes of personal and health information. The PMP is available on icare's website at: https://www.icare.nsw.gov.au/privacy.

2. Scope

This policy applies to:

- Everyone working at icare, including directors, all employees (including part-time and temporary employees), graduates, contingent workers, interns, secondees and volunteers;
- Each claim service provider (CSP and scheme agent who manages claims on behalf of icare; and
- Other service providers that use or hold personal or health information on behalf of icare.

3. Key definitions

3.1 What is personal information?

Personal information is any information or an opinion about an individual, where the

identity of that individual is apparent or could reasonably be ascertained from that information or opinion.

Some examples of personal information include:

- A person's name, home address, email and phone number;
- A person's date of birth, age, gender, height and weight;
- Information about a person's personal or family life, such as marital status, religion or beliefs, or sexuality;
- A person's signature, usernames and passwords;
- Government identifiers (such as Tax File Numbers);
- Identity documents, such as driver's licence details or passport details;
- Financial information, including bank account details, credit card details or information about a person's wealth and investments;
- Employment information, including details of salary and personnel records;
- Information about a person's education and qualifications;
- Information about a person's membership of voluntary or professional bodies, such as a trade union;
- Photographs, video or voice recordings of an individual, where that person can be identified; and
- Information about a person's hobbies or interests.

Opinions about an individual also fall within the scope of personal information. Some examples of opinions include:

- A referee's report about a job applicant;
- Comments made by a supervisor as part of an employee's performance review; and
- Notes that express views about a colleague or a member of the public.

3.2 What is health information?

Health information is personal information or an opinion about any of the following:

- The physical or mental health or disability of an individual;
- An individual's express wishes about the future provisions of health services (to that individual); and
- Health services provided, or to be provided, to that individual.

All personal information collected while providing a health service is also health information (for example, a doctor's clinical notes on a patient).

Health information also includes healthcare identifiers (such as a Medicare number), as well as certain kinds of genetic information about an individual.

Some examples of health information include:

- Information about a physical injury, illness, disease or chronic condition suffered by a person;
- Information about a person's physical disability;
- Information about a mental health condition or mental illness suffered by a person;
- Information about any medical treatment received (or to be received) by a person; and
- An opinion about a person's health, including their future health (for example, a doctor's opinion about a person's likelihood of recovery).

Note that it does not matter whether the relevant health information relates to a past, present or future event.

3.3 When is the identity of an individual apparent or reasonably ascertainable?

A person's identity may be apparent in the information itself. For example, if a person's name is contained in the same record as other information about that person.

A person's identity is reasonably ascertainable if the information could be associated with other information to identify the individual. For example:

- Information that is very specific, such that it could not be referring to anyone else – for example, the CEO of Company X; and
- Information can be linked to other information that would permit an individual to be identified – for example, information linked to a person identified only by a serial number may not be personal information. However, if icare also possessed a record linking serial numbers to individuals, then the information will be personal information.

Care should be taken that any data set that is purportedly anonymised or de-identified cannot reasonably be re-identified.

3.4 What is an incident and a Data Breach?

An **incident** is defined in icare's Incident and Issue Management and Reporting Policy, which at the date of this policy is as follows:

An **incident** is any event which results in an adverse impact on icare, our customers or our people that was caused by:

- A breakdown in processes, controls or systems;
- Human error; or
- An external event.

A **Data Breach** occurs when information held by icare (whether held in digital or hard copy) is subject to unauthorised access, unauthorised disclosure or is lost in circumstances where the loss is likely to result in unauthorised access or unauthorised disclosure.

A **Privacy Data Breach** is when the information subject to the Data Breach is personal or health information.

It does not matter if the Data Breach results from an accidental or deliberate act, or if the cause of the event was internal to icare or external.

Some examples of a Privacy Data Breach include:

- An unauthorised third party (such as a hacker) accesses personal or health information held by icare;
- Personal or health information is unintentionally sent to the wrong recipient (for example, sent to the wrong email address);
- An icare employee who is not permitted to access certain personal or health information, accesses that information (whether deliberately, unintentionally or due to a failure of access controls);
- An icare employee who is only permitted to access certain personal or health information for certain purposes, accesses that information for unauthorised purposes; and
- A device or document containing personal information is lost (for example, a laptop is accidentally left on the train).

An example of a Data Breach that is not a Privacy Data Breach is when a third party (such as a hacker) gains unauthorised access to a confidential document that contains no personal or health information, such as a confidential technical document regarding icare's IT system.

All Data Breaches, whether or not a Privacy Data Breach, should be recorded as incidents in Risk Connect in accordance with the recording and assessment process set out in section 5.3.1 below.

3.5 What is an Eligible Data Breach?

An **Eligible Data Breach** is defined in section 59D of the PPIPA. It is a more serious Data Breach and, briefly stated, occurs where both of the following occur:

- A Privacy Data Breach has occurred (or is likely to have occurred); and
- It is likely that the individual to whom the personal or health information relates would suffer serious harm. Further information on how this "serious harm" assessment must be conducted is set out at section 5.3.3 below.

An Eligible Data Breach also occurs where it cannot be definitively concluded that each of the above conditions have been met, but there are reasonable grounds to suspect that those conditions have occurred.

icare has duties under the PPIPA to respond to Eligible Data Breaches in a particular manner (set out in more detail in section 5 below).

A **Suspected Eligible Data Breach** is a Data Breach that is suspected of being an Eligible Data Breach because from the information currently available an Eligible Data Breach is one of the possible outcomes.

3.6 Other definitions

Authorised Person means any of the following:

- The Chief Executive Officer of icare; and
- A person delegated by the Chief Executive Officer of icare to exercise the functions of that Chief Executive Officer as head of the agency for the purpose of Part 6A of the PPIPA.[1]

The Head of Compliance will exercise the functions of the Authorised Person outlined in this policy unless otherwise directed by the Group Executive, Risk & Governance.

Assessor means an individual appointed by the Authorised Person to carry out an assessment of a data breach to assist the Authorised Person to decide whether it is an Eligible Data Breach. An Assessor may be an icare employee, or an external third party (in either case, who has not been personally involved in the activity giving rise to the breach).

Code of Conduct and Ethics Policy means the code of that name available on icare's website. That code applies to everyone working at icare and provides the guiding principles to support those people in making decisions and choices at their work.

Head of Compliance is the Principal Privacy Officer.

[1] Section 59ZJ of the PPIPA

Incident and Crisis Management Plan means the icare plan of that name which guides relevant icare teams on the steps to be undertaken to manage a disruptive event that impacts icare, allowing for effective incident and crisis management, including assessment and triage, escalation and notification, management by the appropriate team and communication.

Incident and Issue and Reporting Management Policy means the icare policy of that name which applies to everyone working at icare and specifies the principles to be adhered to in order to support effective incident and issue management, including identifying, reporting, investigating, responding, reviewing and closing incidents and accountability for them.

Information and Records Management Policy means the icare policy of that name which outlines the principles to govern how information is created and collected, used and accessed, secured and stored, and retained in accordance with icare's business needs and legal requirements.

Reporting Wrongdoing Policy means the policy of that name available on icare's website. That policy sets out how icare will support and protect staff, volunteers, contractors and subcontractors that come forward with a report of serious wrongdoing. It further explains how to make that report and how icare will deal with it, protecting those who speak up from detrimental action and making sure icare takes appropriate action to investigate or deal with the report.

Responsible Person means the person responsible for reporting and managing an incident under the Incident and Issue and Reporting Management Policy. In Risk Connect, this is the Incident Manager.

4. Policy principles

4.1 What are the IPPs and HPPs that apply?

icare is a public sector agency and is required to comply with the Information Protection Principles and the Health Privacy Principles (together, the "**Principles**").

icare has regard to the Principles when designing and implementing its services, processes and systems, to ensure that they are built into icare's way of doing business.

All icare employees must comply with the Principles when collecting and handling personal or health information.

Summary of relevant Principles

A reference to information in the following table means personal and health information unless specified otherwise.

Title	Summary
Collection	We must only collect information if it is necessary for a purpose that is directly related to icare's functions and activities. We must make sure that any information we collect is relevant for our purposes, is accurate, up to date and is not unreasonably intrusive. Where practical, we must collect information directly from the person to whom the information relates (or their authorised representative). Where collecting health information from a third party we must take reasonable steps to notify the person that this has occurred. We must provide a Privacy Collection Notice to all individuals at the time that their information is collected, or as soon as practicable after collection. The Privacy Collection Notice must explain what information is being collected, why we are collecting the information, how it will be used, who it will be disclosed to, whether the information is required by law, the consequences of not providing the information, how the information can be accessed and corrected.
Consent	When relying on consent for use or disclosure of an individual's information, we must ensure that: • The individual is fully informed of how their information will be used and/or who it will be disclosed to; • Consent is freely given; • The request for consent is current and specific; and • The individual has capacity to consent.
Retention and Disposal	Information must not be kept for longer than necessary to fulfil the purpose for which it was collected and must be securely disposed of once that purpose is fulfilled. Where information is required to be disposed of, it must be disposed of securely. No document may be disposed of without proper authority. icare (and each scheme managed by icare) is required to comply with the relevant retention and disposal authorities in place and issued by the State Records NSW. Appropriate meta-data must be retained after disposal including information such as the name of the file, the dates of creation and disposal, the disposal authorisation, disposal method etc. Further information is set out in icare's Information and Records Management Policy.
Access and correction	We must allow the person to whom the personal and health information relates to access it without excessive delay or expense. We must allow the person to whom the personal and health information relates to update, correct or amend their personal information. Further information is set out on the "Your privacy" page at the following address: https://www.icare.nsw.gov.au/privacy/your-privacy.
Use	We must take steps to ensure that information is relevant, accurate, up to date, complete, not excessive and not unreasonably intrusive before using it. We must only use personal and health information for the purpose it was collected. Generally, consent is needed to use the information for another purpose.

Title	Summary
Disclosure	We must only disclose personal and health information in the following circumstances: • The person consented to the disclosure; • When the information was collected, the person was told that the information would be disclosed and the disclosure relates to the purpose for which the information was collected; • It is for a directly related purpose to which the information was collected, and the person would expect the disclosure and not unreasonably object to it; • It is to prevent or lessen a serious or imminent threat to a person's health or safety; or • Disclosure of the information is otherwise expressly permitted by law. Sensitive personal information such as ethnic and racial origins, political opinions, religious beliefs cannot be disclosed without consent unless it is to prevent or lessen a serious or imminent threat to a person's health or safety.
Transborder Data Flows	We must have appropriate measures in place to ensure the transfer of personal or health information outside of NSW is done in compliance with legal requirements.
Anonymity, Unique Identifiers and Health Information Linkages	We must allow people to receive services from us anonymously, where it is lawful and practical. In relation to health information, we may only assign unique identifiers (for example, a number) to an individual's health information if it is reasonably necessary to enable us to carry out any of our functions efficiently. We must not include health information in a health records linkage system without the individual's consent.

4.2 Privacy Impact Assessment (PIA)

When designing and implementing new projects or initiatives or where there are changes to projects or existing processes and / or systems that involve the handling of personal or health information, a Privacy Impact Assessment (PIA) must be undertaken.

A PIA assesses the impacts on privacy on a project, technology, product, service, policy, program or other initiative and assist, in consultation with stakeholders, in identifying mitigating actions to manage associated privacy risks.

A PIA assists to incorporate a 'privacy by design' approach and supports effective compliance with privacy laws.

A PIA provides an opportunity for privacy risks to be avoided or mitigated by ensuring a project complies with the law, meets community expectations, and is as least privacy-invasive and most privacy-enhancing as possible.

A PIA should be conducted at the design stage of a new system or program by the relevant service line or business unit in collaboration with the 1st Line Risk team. The PIA will be reviewed and endorsed by the 2nd Line Compliance team and, where required, the Legal team and any recommendations made must be considered and where practical adopted.

4.3 Penalties for non-compliance with Information Protection and Health Privacy Principles

Breaches of this policy arising from a deliberate, intentional or negligent act or omission may result in disciplinary action up to and including termination of employment, depending on the circumstances, severity and impact of the breach.

Any instance of non-compliance with this policy must be managed and reported in accordance with the Incident and Issue and Reporting Management Policy.

To the extent relevant, non-compliance with this and other policies, such as the Code of Conduct and Ethics Policy, could also be reported under icare's Reporting Wrongdoing Policy.

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.

If employees are uncertain as to whether certain conduct may breach icare's privacy obligations, they should seek the advice of the Privacy team.

5. Incidents and Eligible Data Breaches

5.1 Overview

Effective management of incidents and Data Breaches is an essential part of meeting icare's compliance obligations, improving customer experience, and maintaining community trust in how icare deals with people's personal and health information.

Under the PPIPA, Eligible Data Breaches must be notified to the Privacy Commissioner and affected individuals unless an exception applies. These are called Eligible Data Breaches. Not all Privacy Data Breaches are Eligible Data Breaches.

This section of this policy is intended to provide guidance on what to do if a Privacy Data Breach occurs, and when (and how) an Eligible Data Breach is required to be notified to the Privacy Commissioner and affected individuals.

icare has the following measures in place to prepare for a Data Breach:

- Annual testing and review of this Policy.
- All people working at icare are required to complete annual mandatory privacy training to ensure they know and understand their privacy obligations and how to identify and report a suspected Data Breach.
- A privacy awareness strategy to ensure that people working at icare and relevant suppliers are aware of their responsibilities under this Policy.
- Third-party contracts include, where relevant, provisions for reporting, managing Data Breaches and relevant mandatory training.
- Post-incident reviews are undertaken to assess icare's response to the Data Breach and the effectiveness of this Policy.

5.2 Preventing Privacy Data Breaches

It is within the power of every person working at icare to minimise the risk of a Privacy Data Breach occurring by complying with this Policy, as well as the policies specified in section 7 below, and promptly raising any concerns or issues with their People Leader or 1st Line Risk team.

Compliance with this policy ensures that appropriate safeguards are in place before personal or health information is collected, used by, disclosed to, or accessed by third parties.

Cyber security training and awareness is provided to people working at icare to prevent Data Breaches.

5.3 Reporting and responding to a Privacy Data Breach

The five key steps to respond to a Privacy Data Breach are as follows:

Each step is set out in further detail below. The first four steps should be carried out concurrently where possible. The last step provides recommendations for longer-term solutions and prevention strategies.

5.3.1 Step 1: Initial report and triage

icare may become aware of a Data Breach by its own employee or by being notified by a customer, service provider or a member of the public or other third party.

All suspected or potential Data Breaches must be recorded as an incident in Risk Connect[2] within two business days of an icare employee becoming aware of it. For privacy data breaches these must be recorded as a "Privacy/Data" incident. Significant / urgent incidents which involve a large volume of personal/health information, or a cyber attack are expected to be reported and escalated immediately on identification to the Head of Compliance.

If a person working at icare is unsure if an incident is a privacy data breach or a Suspected Eligible Data Breach, they should contact their People Leader or their 1st Risk team for further advice.

Often icare will be unable to determine if a Data Breach is a Privacy Data Breach until after the breach is investigated. Accordingly, if it is unclear that personal or health information is the subject of the Data Breach, then the Data Breach must be recorded as a Privacy Data Breach until determined otherwise.

Wherever there is uncertainty about whether a Privacy Data Breach is a Suspected Eligible Data Breach the incident should be recorded as a Suspected Eligible Data Breach and notified to the Authorised Person in accordance with this policy.

Members of the public or others outside of icare can report a suspected Data Breach

[2] Risk Connect is the name given to icare's internal governance, risk and compliance system. One use of Risk Connect is to record incidents. Being an internal tool, Risk Connect is not accessible by the public.

involving personal and/or health information held by icare by emailing icare at: privacy@icare.nsw.gov.au

Initial investigation

After a Data Breach has been recorded in Risk Connect, the person responsible for managing the incident under the Incident and Issue Management and Reporting policy ("**Responsible Person**") must, without delay, investigate and keep records in relation to each Data Breach in accordance with that policy.

The Responsible Person must escalate a Suspected Eligible Data Breach or actual Eligible Data Breach in accordance with section 5.3.3 below.

5.3.2 Step 2: Contain the breach

icare must, without delay, take all reasonable efforts to contain any Data Breach and mitigate the risk of harm to affected individuals.

The Responsible Person must co-ordinate the initial containment steps (or delegate responsibility to another appropriately qualified employee, or a member of a Data Breach Response team, where convened).

How a Data Breach is contained will depend on its nature. It may be appropriate to seek the expertise of other icare employees (including IT or Legal) or external service providers (such as, cyber forensics or legal expertise).

If the Data Breach involves third party service providers, icare must, without delay, consider what directions it may need to give those providers to help contain and mitigate the Data Breach. The Responsible Person must co- ordinate the response to the Data Breach (or delegate this responsibility to another icare employee), including with the icare data breach response team relevant in the circumstances.

The response may include retrieval and/or deletion of lost data, ceasing unauthorised access, shutting down or isolating affected systems, or consulting with other entities that jointly hold data with icare.

All evidence of the Data Breach should be collected and preserved to allow for the cause of the breach to be determined and to allow measures to be taken to prevent its reoccurrence.

5.3.3 Step 3: Assess and mitigate

After an incident is recorded in Risk Connect it will be promptly evaluated by the Responsible Person and, if assessed as a Suspected Eligible Data Breach, then this must be immediately reported to the Compliance team at privacy@icare.nsw.gov.au.

Although the procedure for reporting an incident in Risk Connect applies, a person working at icare may choose to also report a Suspected Eligible Data Breach directly to the Head of Compliance, such as when an urgent Suspected Eligible Data Breach occurs.

On receipt of a report of a Suspected Eligible Data Breach the following steps will be taken:

- The Compliance team will notify the Authorised Person of the receipt of the report; and
- The Authorised Person will ensure that the incident has been contained and appoint an Assessor. An Assessor may be an employee, an employee of another NSW Government agency or an external third party (in each case provided the person was

not otherwise involved in the Data Breach)
- The Assessor will:
    - Seek further information from the Responsible Person, and provide advice on any additional containment measures not already employed, or mitigation measures recommended; and
    - Immediately commence an assessment of the Suspected Eligible Data Breach (namely, whether it is more likely than not that the affected individual(s) would suffer serious harm as a result of the breach taking into account the factors in s. 59H of the PPIP Act). The assessment must be carried out expeditiously.
- The Assessor is to prepare an assessment report on the findings of the assessment and the reasons for the findings including as to whether the Assessor considers that the Suspected Eligible Data Breach is an Eligible Data Breach, or there are reasonable grounds to believe it is an Eligible Data Breach;
- The Assessor is to provide the assessment report to the Authorised Person as soon as possible and in accordance with the timeframes stipulated in this Policy.

The Authorised Person is responsible for determining whether an Eligible Data Breach has occurred (or whether there are reasonable grounds to believe an Eligible Data Breach has occurred).

The Authorised Person may determine upon receipt of a report of a suspected Eligible Data Breach that it is necessary to convene a multi-disciplinary response team, known as a Data Breach Response team, to manage icare's response to a Suspected Eligible Data Breach. Determining whether escalation to a response team is required will include consideration of:
- The sensitivity of information involved;
- The number of individuals affected;
- Any suspected external exposure of individuals' personal information;
- Any suspected unlawful activity;
- Any unauthorised use or disclosure (whether internal or between agencies) of certain categories of individuals' personal information – for example if users of a particular service are particularly vulnerable; and
- The risk of harm to the individuals involved and the nature of any potential harm.

The Authorised Person may decide to consult with internal and external expertise or resources to make this decision including icare Legal, although the responsibility for deciding remains with the Authorised Person.

Timeframes for determining an Eligible Data Breach

The Authorised Person must decide whether there has been an Eligible Data Breach (or whether there are reasonable grounds to believe an Eligible Data Breach has occurred) within 30 calendar days of the date the icare employee who identified it became aware that there were reasonable grounds to suspect an Eligible Data Breach had occurred. In practice, this timeframe will be triggered once the Responsible Person forms the view that it is a Suspected Eligible Data Breach. Where this is in doubt it should be recorded as a Suspected Eligible Data Breach.[3]

The Assessor is to provide the assessment report to the Authorised Person as soon as possible and no later than seven business days before the 30 calendar day period ends.

[3] Section 59H of PPIPA

If the Assessor believes the assessment cannot be concluded within the 30-calendar day period, then the Authorised Person may extend this time for completion of the assessment for a period reasonably required for the assessment to be concluded. Further extensions may also be made but must be approved by the Group Executive, Risk & Governance.

All extensions must be reported to the IPC by the Authorised Person. What is serious harm?

Serious harm includes serious physical, psychological, emotional, financial, or reputational harm.

Examples of serious harm include:

- Identity theft – where identity documents have been compromised;
- Financial loss – where credit card details have been compromised;
- Physical harm – where a person has an abusive ex-partner and the person's contact details are to be kept secret; and
- Psychological or emotional harm – where sensitive information about a person's health is compromised.

What information must be considered?

The serious harm assessment must be made based on:

- The information that has been accessed or disclosed in the privacy incident; and
- Any other relevant information icare is aware of in respect of the affected individual.

For example, if icare is aware that a person affected by a privacy incident suffers a particular mental illness, then this should be considered in the serious harm assessment, even if the information compromised by the privacy incident did not include information about that person's mental illness.

However, icare is not required to seek out further information about the personal circumstances of an affected individual.

What factors must be considered in assessing the likelihood of serious harm?

The following factors must be considered to assess the likelihood of serious harm:[4]

- The types of personal or health information involved;
- The sensitivity of the personal or health information involved;
- Whether the personal or health information is or was protected by security measures;
- The persons to whom the unauthorised access to, or unauthorised disclosure of, the personal or health information was, or could be, made or given;
- The likelihood of those persons intending to cause harm, or circumventing security measures protecting the information;
- The nature of the harm that has occurred or may occur; and
- Any other matter specified in the Privacy Commissioner's guidelines.

An Eligible Data Breach only occurs where serious harm is **likely**. "Likely" means more probable than not (rather than merely possible).

[4] Section 59K of the PPIPA

Additional consideration where personal or health information is lost

In the situation where the incident involves personal or health information being lost (for example, a device accidentally left on the train), the serious harm assessment must also include an assessment of the likelihood that there will be unauthorised access or disclosure of personal or health information.

For example, where a device has both password and two-factor authentication security, and icare's IT security team can remotely wipe the device, it may be possible to conclude that there is a low likelihood that there will be unauthorised access or disclosure of personal or health information on that device, because of that device's security measures.

5.3.4 Step 4: Notify

If the Authorised Person decides that an Eligible Data Breach has occurred (or there are reasonable grounds to believe an Eligible Data Breach has occurred), then the notification process is triggered. There are four elements of the notification process:

1. Notify the Privacy Commissioner. The Authorised Person must notify the Privacy Commissioner immediately after an Eligible Data Breach is identified using the IPC approved form.
2. Consider any exemptions. The Authorised Person must make a recommendation to the Group Executive, Risk & Governance, as to whether any of the six exemptions to notifying of an Eligible Data Beach apply[5]. Where the Group Executive, Risk & Governance determines that the exemption applies icare is not required to notify affected individuals.
3. Notify individuals: Unless an exemption applies, the Authorised Person is to co-ordinate the notification of affected individuals or their authorised representative as soon as practicable (see "When to notify" below).
4. Provide further information to the Privacy Commissioner as required.

icare recognises that notification to individuals or organisations affected by a Data Breach can assist in mitigating any damage for those affected. Notification demonstrates a commitment to open and transparent governance, consistent with icare's values.

If a Data Breach is not an Eligible Data Breach, icare may still consider notifying individuals and organisations of the breach. Notification in appropriate cases demonstrates a commitment to open and transparent governance, consistent with icare's values.

Notification should be undertaken promptly to help avoid or lessen the damage by enabling the individual and/or organisation to take steps to protect themselves. The PPIPA requires icare to take reasonable steps to notify affected individuals of an Eligible Data Breach as soon as practicable (see "When to notify" below).

The method of notifying affected individuals and organisations will depend in large part on the type and scale of the breach, as well as immediately practical issues such as having contact details for the affected individuals and organisations. Some of the considerations are set out below.

When to notify

The PPIPA requires icare to take reasonable steps to notify affected individuals of an Eligible Data Breach as soon as practicable. What being notified as soon as practicable means will depend on the circumstances, but typically means notifying when notice is capable of being put into practice with the available means.

The Privacy Commissioner's guidelines highlight that:

- Timely notification is important to help individuals affected by a breach take steps to limit or mitigate the risks of misuse or further exposure;
- icare should avoid undue delay and work to make affected individuals aware of the breach as soon as possible;
- icare should carefully balance speedy notification to individuals with ensuring that people are provided with reliable and accurate information about the breach;
- Notifications should provide recipients with an accurate sense of what risks may arise for them and what practical measures they can take to protect themselves. An inaccurate notification could cause more harm than good, such as unnecessary anxiety and fail to enable those affected to take protective action. If icare is not yet able to provide meaningful detail in a notification, it may be too early to provide it; and
- For complex breaches or where significant numbers of individuals are affected, icare may need to consider a phased approach to notification, such as notifying in tranches based on the level of risk posed to the individual or the sensitivity of the information involved in the data breach.

Where individuals affected by an Eligible Data Breach cannot be notified, icare will consider issuing a public notification on our website (see "How to notify" below).

How to notify

Generally, affected individuals and organisations should be notified directly (by telephone, letter, email or in person).

In some circumstances, it may not be practical for icare to notify affected individuals directly. For example, where the contact information of affected individuals and organisations is unknown, or where direct notification is prohibitively expensive or could cause further harm (for example, by alerting a person who stole the laptop as to the value of the information contained). When this occurs, the Group Executive, Risk & Governance may approve a public notification (such as information being published on icare's website, a public notice in a newspaper, or a media release). A record of any public notification of an Eligible Data Breach will be published on icare's website and recorded on the Public Data Breach Notification Register for a period of at least twelve months.

What to say

The PPIPA sets out the information that must be included in notifications to individuals, including:

- The date the breach occurred;
- A description of the breach;
- How the breach occurred;
- The type of breach that occurred;
- The personal information included in the breach;
- The amount of time the personal information was disclosed for;
- Actions that have been taken or are planned to secure the information, or to control and mitigate the harm;
- Recommendations about the steps an individual should take in response to the breach information about complaints and reviews of agency conduct;
- The names of agencies that were subject to the breach; and
- Contact details for further information about the breach.

Other notification obligations

The Authorised Person will also consider whether other organisations, agencies or regulatory bodies should be notified of a Data Breach (whether or not it is an Eligible Data Breach). Depending on the circumstances this could include:

- NSW Police Force and/or Australian Federal Police, where icare suspects a Data Breach is a result of criminal activity.
- The Independent Commission Against Corruption (ICAC) where icare suspects a Data Breach is a result of corrupt conduct.
- Cyber Security NSW, the Office of the Government Chief Information Security Officer and The Australian Cyber Security Centre, where a Data Breach is a result of a cyber security incident.
- The Office of the Australian Information Commissioner, where there are notification requirements under the Privacy Act 1988.
- Any third-party organisations or agencies whose data may be affected.
- Financial services providers, where a Data Breach includes an individual's financial information.
- Professional associations, regulatory bodies or insurers, where a Data Breach may have an impact on these organisations, their functions and their clients; and
- The Australian Cyber Security Centre where a Data Breach involves malicious activity from a person or organisation based outside Australia.

The Authorised Person must consult with Legal and the Group Executive Risk & Governance before making any of the above notifications.

Incidents assessed as not being an Eligible Data Breach

If the Authorised Person determines that an Eligible Data Breach has not occurred, then icare is not required by the PPIPA to notify either the Privacy Commissioner or affected individuals about the Data Breach.

In this situation, the Authorised Person should decide whether the Privacy Commissioner or affected individuals should be notified on a voluntary basis. The Authorised Person must consult with Legal and the Group Executive Risk & Governance before making any notification on a voluntary basis.

Voluntary notification of individuals should only be made in exceptional circumstances, such as when the benefits of voluntary notification materially outweigh the potential harm. This is because notifying individuals about a Data Breach that poses little or no risk of serious harm can cause unnecessary anxiety and inconvenience. If icare notifies individuals of Data Breaches when not required to do so under the PPIPA, then this could lead to people being desensitised to these kinds of notices, so they don't take a notification seriously, even when there is a real risk of serious harm. These factors should be considered when deciding whether to notify individuals on a voluntary basis.

Interaction with the Incident Review Panel (IRP) and Significant Matter Notification Requirements

A privacy or information breach is a significant matter, and requires escalation to the Incident Review Panel prior to notification to the State Insurance Regulatory Authority (SIRA), if it arises during a regulated entities scheme related insurance business (in whole or part) and icare:

- Gives a statement to the Office of the Australian Information Commissioner (OAIC)

under section 26WK of the Commonwealth Privacy Act 1988 (Privacy Act);
- Receives notice of a declaration by OAIC under section 26WQ of the Privacy Act;
- Receives notice of a direction by OAIC under section 26WR of the Privacy Act;
- Gives notice to the NSW Privacy Commissioner (NSWPC) under Part 6A of the NSW Privacy and Personal Information Protection Act 1998 (PPIP Act);
- Receives notice from the NSWPC under section 59Y of the PPIP Act; and
- Makes a security breach notification in the event of a significant cyber incident to Cyber Security NSW in accordance with the NSW Cyber Security Policy.

The Incident Review Panel process is triggered by the reporting of an incident in Risk Connect and runs concurrently with any assessment under this Policy.

5.3.5 Step 5: Review

After a Data Breach has been resolved, it may be necessary to conduct a review to assess how it occurred, and what changes may be made to prevent reoccurrence.

This should include a review and remediation of:
- The internal controls in place;
- Policies and procedures;
- Staff skills and training;
- Contractual obligations with contracted service providers; and
- Any other material issues relevant to the Data Breach.

The Responsible Person must ensure that a post-incident review, including an assessment of how icare responded to the Data Breach, must be carried out:
- For Eligible Data Breaches;
- Where a Privacy Data Breach arose because of a malicious act;
- Where systemic shortcomings in icare's processes or systems have been identified; and
- In any other situation as determined by the Authorised Person or the Group Executive Risk & Governance.

If a post-incident review raises any issues or concerns about the effectiveness of this Policy, this should be reported to the Group Executive Risk & Governance.

5.4 Internal Eligible Data Breach Register

The Authorised Person must ensure that all Eligible Data Breaches are recorded on icare's internal Data Breach Incident Register as soon as practicable by the Privacy team and within 2 business days of the determination that there has been an Eligible Data Breach. The Head of Compliance is responsible for ensuring that the Data Breach Incident Register is up to date and accurate.

5.5 Communications Strategy

Depending on the nature and/or scale of the Eligible Data Breach, a communications strategy may need to be implemented by icare. icare's Incident and Crisis Management Plan contains roles and responsibilities for managing communications when an incident occurs.

6. Roles and responsibilities

Role	Responsibilities
All Employees	• Always comply with the requirements of this policy and related policies and procedures. • Actively consider privacy risk in business processes and related activity, take action to mitigate or escalate issues if necessary. • Implement and/or support the implementation of controls to mitigate privacy risk. • Complete mandatory privacy awareness and related training. • Report and/or escalate all incidents, data breaches and 'near misses' and issues in Risk Connect in accordance with this Policy.
Responsible Person	• Maintain overall responsibility for the timely and quality reporting and management of incidents under the Incident and Issue and Reporting Management Policy. • Preliminarily assess and report any Suspected Eligible Data Breaches in accordance with this Policy. • Coordinate containment steps (or delegate responsibility to another suitably qualified icare employee, or member of a Data Breach Response team). • Escalate a Suspected Eligible Data Breach or actual Eligible Data Breach in accordance with this Policy. • Gather further information about Privacy Data Breaches to assist an Assessor • Conduct post-incident reviews.
Authorised Person	• Appoint an assessor to undertake an assessment of a suspected Eligible Data Breach in accordance with the MNDB scheme under the PPIPA. • Determine, considering an assessor's advice, whether there has been an Eligible Data Breach. • Oversee communication with the NSW Privacy Commissioner and the Office of the Australian Information Commissioner in relation to Data Breaches. • Notify Eligible Data Breaches to the NSW Information Privacy Commissioner or the OAIC as required.
Board	• Review and approve this policy annually. • Set the tone at the top for the culture and objectives of this policy within icare. • Accountable for the effectiveness of this policy and its application. • Complete mandatory privacy awareness and related training.
Board Risk Committee	• Oversee the effective implementation of this policy and icare's approach to privacy management. • Seek assurance that icare has adequate resources and arrangements for effective privacy management. • Review and endorse this policy prior to Board approval. • Complete mandatory privacy awareness and related training.
Group Executive – Risk & Governance (in addition to above)	• Approve reliance on any exemption for notifying affected individuals; the granting of a second extension of time for an Assessment to be completed; the public notification of data breaches; and the provision of any statement to the IPC under s. 59Y of the PPIP Act. • Oversee the regular review of this policy and icare's Privacy Management Plan and recommend changes and updates for approval by the Board as appropriate. • Report to senior management and the icare Board Risk Committee on confirmed Eligible Data Breaches and the overall management of privacy risk across icare.

Role	Responsibilities
Group Executives	• Drive a culture of compliance with this policy and raise awareness of robust and pro-active privacy management practices. • Accountable for implementing this Policy, managing privacy risk, remediation of privacy incidents and the ongoing adherence to the policy within their businesses. • Ensure all people working in their business unit have completed all privacy training and understand their privacy obligations.
Legal	• When requested, provide legal advice on matters relevant to this policy and on icare's management of Data Breaches pursuant to the MNDB scheme requirements. This includes for: • 1. The use of an exemption from notification to individuals affected by an Eligible Data Breach. • 2. An extension of time for completion of an assessment. • 3. Public notification of a data breach. • 4. Data breaches that involve triggers for escalation.
First Line Risk	• Support the business in complying with this Policy, including promoting an understanding of privacy obligations, identifying privacy risk, undertaking PIAs and implementing management controls. • Co-operate with the Compliance team in recording and assessing incidents and data breaches in accordance with this Policy.
Second Line Risk team	• Provide support and advice to the business in managing privacy risks, issues and incidents.
Second Line Compliance team)	• Provide advice on Privacy Data Breaches/Suspected Eligible Data Breaches escalated by the Responsible Person, 1st Line Risk, or other staff. • Notify the Authorised Person of all suspected Eligible Data Breaches • Act as the Assessor for Suspected Eligible Data Breaches subject to the direction of the Authorised Person and provide advice to the Authorised Person as to the required determination within the prescribed timeframes. • Provide advice to the Group Executive, Risk & Governance on icare's reliance on any exemption from notification of Eligible Data Breaches, or the need for a further extension of time to make a notification under the MNDB Scheme. • Manage/coordinate the investigation and resolution of escalated privacy complaints and Privacy Internal Review applications which may arise in connection with or independently of a Privacy Data Breach. • Manage updates to icare's internal and published registers of Data Breaches. • Provide advice on privacy queries, issues and incidents escalated from 1st Line Risk. • Provide advice and support to 1st Line Risk and the business on undertaking PIAs. • Respond to and manage information access requests under the PPIPA and HRIPA. • Monitoring of privacy risk and the operation of the privacy management program across icare. • Provide support, challenge and advice to the business in managing privacy risks, issues and incidents.
Head of Compliance (Principal Privacy Officer)	• Develop icare's statutory Privacy Management Plan for approval by the Group Executive Risk & Governance. • Monitor legislative and regulatory changes which may impact the way icare processes and manages personal information and advise icare on its application.

Role	Responsibilities
	• Monitor the currency and effectiveness of this policy and compliance with it and support the Group Executive Risk & Governance with reporting to icare governance committees. • Take a proactive management approach to reducing the number and severity of privacy incidents • Provide guidance and advice on the development of processes and procedures for management of privacy incorporating a privacy by design approach • Establish the requirements for completing privacy impact assessments. • Endorse PIAs and seek endorsement from Legal where appropriate • Develop training and awareness for privacy related policies and procedures. • Develop relationships with management, staff and risk coordinators to influence and foster a compliance culture.

7. Related Policies or Procedures

This policy should be read in conjunction with:

- Code of Conduct and Ethics Policy
- Incident and Crisis Management Plan
- Cyber Incident Response Plan
- Incident and Issue Management and Reporting Policy
- Information and Records Management Policy

8. Contact for Enquiries and Feedback

The Compliance team can be contacted by emailing privacy@icare.nsw.gov.au.

9. Version Control and Document History

Document Name & Version	Privacy and Data Breach Policy V2.0
Document owner	Group Executive Risk & Governance
Approving Authority	Board
Last Approval Date	25 November 2024
Review Frequency	Annually

Version	Author	Change Summary	Approval Date
v1.0	Principal Privacy Officer	Updated policy to comply with amendments under the *Privacy and Personal Information Protection Act 1998* (NSW).	27 November 2023
V2.0	Acting Head of Compliance	Main updates following policy review:	25 November 2024

Version	Author	Change Summary	Approval Date
	(Principal Privacy Officer)	• Amendments of roles and responsibilities to incorporate changes to operating model and reflect delegations. • Introduction of requirement for PIAs to be mandatory for all projects and initiatives involving the handling of personal and health information. • Amended to clarify process for identifying, assessing and notification of Eligible Data Breaches under the MNDB scheme.	