Cancer Institute NSW

# Data Breach Policy

**Data Governance**

Version 1.0 | 08 April 2024

NSW GOVERNMENT

| | | | |
|---|---|---|---|
| **Document Title:** | Data Breach Policy | | |
| **Summary:** | Outlines the minimum requirements and standards to ensure data breaches involving personal or health information are managed appropriately, in a timely manner, and in compliance with the obligation to report eligible data breaches to the NSW Privacy Commissioner and individuals affected by a data breach under the Mandatory Notification of Data Breach Scheme. | | |
| **Date of Issue:** | *30-Aug-24* | **Next Review Date:** | *28-Aug-26* |
| **Status:** | Active | **Review Cycle:** | Every 2 Years |
| **Contact Officer:** | Chief Data Officer | | |
| **Applies To:** | All staff and contractors of all Divisions of the Cancer Institute NSW. | | |
| **References:** | **Policy, Procedures and Guidelines:**<br>• Data Breach Management – Standard Operating Procedure (E19/18163) – rescinded<br>• Data Breach Management Incident Report (E21/05954)<br>• Information Security Policy (E07/26801)<br>• Risk Management Procedure (E20/05203)<br>• Records and Information Management Policy (E06/10927)<br>**NSW Government:**<br>• Privacy and Personal Information Protection Act 1998 (PPIP Act)<br>• Health Records and Information Privacy Act 2002 (HRIP Act)<br>• NSW Health Policy Directive – Data Breaches involving Personal or Health Information (PD2023-040)<br>• NSW Health Privacy Manual for Health Information<br>• NSW Health Data Governance Framework (GL2019_002)<br>• NSW Health – Electronic Information Security (PD2020_046)<br>• NSW Health – Privacy Management Plan (IB2023_012)<br>• NSW Government Cyber Security Policy<br>• Information and Privacy Commission NSW – Guidelines on the assessment of data breaches under Part 6A of the PPIP Act<br>• Information and Privacy Commission NSW – Fact Sheet – Mandatory Notification of Data Breach Scheme<br>• Information and Privacy Commission NSW - Data Breach Self-Assessment Tool for Mandatory Notification of Data Breach<br>**Australian Government:**<br>• Data Breach Preparation and Response – A Guide to Managing Data Breaches in Accordance with the Privacy Act 1988 (Cth) | | |
| **Replaces** | E19/18163 - Data Breach Management – Standard Operating Procedure | | |

| **Version and Change History** | **Version** | **Who** | **Date** | **What** |
|---|---|---|---|---|
| | 1.0 | *Privacy Contact Officer* | *15/11/2023* | *E19/18163 has been rescinded and replaced by a new Data Breach Policy to reflect amendments to the Privacy and Personal Information Protection Act 1998 (PPIP Act). Part 6A of the PPIP Act provides for a mandatory notification of data breach scheme, with effect from 28 November 2023. Agencies are to provide mandatory notifications to affected individuals in the event of an eligible data breach, notify* |

| | | | | |
|---|---|---|---|---|
| | | | | *the NSW Privacy Commissioner, establish and maintain an incident register and public notification register, and comply with other data management requirements.* |
| **Reviewer(s)** | **Version** | **Who** | **Date** | **What** |
| | | *Chief Data Officer* | *8/04/2024* | *Approved* |
| | | | | |
| | | | | |
| **Approvals** | **Version** | **Who** | **Date** | **Record** |
| | 1.0 | *Chief Executive Officer* | *29/08/2024* | *E24/15666-2.* |
| | | | | |

# Contents

# 1. Introduction

## 1.1 Overview

The Cancer Institute NSW (the Institute) has an obligation under the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) to put in place reasonable security safeguards and to take reasonable steps to protect the personal and health information that it holds.

Data breaches can result in serious harm to affected individuals and the Institute. How the Institute responds to data breaches impacts the reputation of the New South Wales (NSW) Health system, and the degree to which patients, staff and other third parties trust NSW Health with their personal and health information.

Compliance with the PPIP Act, HRIP Act or other relevant legislation (e.g. Public Health Act), and related NSW government, NSW Health or Institute policies, including NSW Health's Privacy Manual for Health Information and the Institute's Information Security Policy (E07/26801), ensure the data the Institute holds are protected.

Each data asset must have in place processes to protect the privacy and confidentiality of data through access management and security controls. This includes ensuring that the data is appropriately secured, backed up and disposed of according to agreed and documented protocols. Data must only be disclosed for the purpose for which it is collected.

This policy is aligned with the NSW Health Policy Directive on Data Breaches involving Personal or Health Information (PD2023_040) and the Information and Privacy Commission's Statutory Guidelines on the assessment of data breaches under Part 6A of the PPIP Act.

Amendments have been made to the PPIP Act which impact the responsibilities of NSW Health organisations under the PPIP Act. The changes include creating a Mandatory Notification of Data Breach Scheme (MNDB Scheme) which requires all NSW Health organisations to notify the NSW Privacy Commissioner and affected individuals of data breaches involving personal information (including health information) that are likely to result in serious harm (unless certain limited exemptions apply).

It also requires NSW Health organisations to satisfy other data management requirements, including an obligation to maintain an internal data breach incident register, an external register of public notifications, and have a publicly accessible data breach policy.

## 1.2 Purpose

The purpose of this document is to outline the procedure to be followed in the event of an actual, suspected or a near miss data breach. It also outlines the minimum requirements and standards for the Institute under the MNDB Scheme to ensure data breaches involving personal or health information are managed in compliance with the obligation to report eligible data breaches to the NSW Privacy Commissioner and affected individuals.

The Institute may also be subject to other mandatory notification obligations in relation to the management of data breaches when responding to a data breach under this Policy (a non-exhaustive list of additional reporting NSW Health obligations is outlined in section 5).

This document is complementary to the *NSW Health Data Governance Framework* (GL2019_002), which outlines the roles and responsibilities involved in data governance and the structures in place to ensure effective and consistent management of the data assets of NSW Health. It is also complementary to the NSW Health Policy Directive *Electronic Information Security* (PD2020_046) which outlines the responsibility to uphold confidentiality and protect information entrusted to them to include reporting any information security concerns, events or incidents to eHealth NSW.

### 1.3 Scope

This procedure applies to all staff, contingent workers and contractors of all Divisions and business units in the Institute.

## 2. Policy Statement

The Institute must make all reasonable attempts to contain and mitigate harm arising from a data breach involving personal or health information held by the Institute, and notify the Privacy Commissioner, the Ministry of Health, and affected individuals, where the notification is required and appropriate.

The purpose of this policy is to provide guidance to Institute staff on data breaches of data held by the Institute in accordance with the requirements of the PPIP Act.

This policy sets out how the Institute will respond to data breaches involving personal information. The Institute acknowledges that not all data breaches will be eligible data breaches but regardless the Institute will take all data breaches seriously. The policy details:

- what constitutes an eligible data breach under the PPIP Act
- roles and responsibilities for reporting, reviewing and managing data breaches
- the steps involved in responding to a data breach and reviewing systems, policies and procedures to prevent future data breaches.

Amendments to the PPIP Act in 2023 impact the responsibilities of NSW Health organisations under the PPIP Act. The changes include creating a Mandatory Notification of Data Breach Scheme which requires all NSW Health organisations to notify the NSW Privacy Commissioner and affected individuals of eligible data breaches involving personal information (including health information) that are likely to result in serious harm (unless certain limited exemptions apply).

It also requires the Institute to satisfy other data management requirements, including an obligation to maintain an internal data breach incident register, an external register of public notifications, and have a publicly accessible data breach policy.

## 3. Roles and Responsibilities

### 3.1 All Institute Staff

All staff members have a responsibility to identity and report actual or suspected data breaches.

All staff are responsible for the following:

- report a data breach to their manager immediately and, where practicable, take appropriate action to contain the breach
- Participate in breach assessment teams, if required
- Implement and/or follow containment, corrective and preventive actions, if required
- Preserve the integrity of evidence

### 3.2 Chief Executive Officer

The Chief Executive Officer (CEO) has ultimate responsibility and accountability for the Institute's response and management of data breaches. This includes making all reasonable attempts to contain the breach and mitigate the harm done by the breach.

Where, after assessment, a data breach is determined as being an eligible data breach under the MNDB Scheme, the CEO must immediately notify the NSW Privacy Commissioner of the breach.

Following an eligible data breach, the CEO is responsible for determining whether certain individuals are notified, whether a public notification is to be made, or whether the organisation is exempt from notifying affected individuals.

Under the MNDB Scheme, there are several powers conferred to chief executives. While these powers may be delegated, the CEO must ensure a local decision to delegate powers under the MNDB Scheme are only to those staff members with appropriate seniority, expertise, and capability in responding to data breaches, and who have a sound understanding of the applicable privacy legislation.

The CEO and Chief Data Officer can veto any actions or mitigations in response to a data breach.

### 3.3 Managers

Managers at all levels are responsible for escalating reports of actual or suspected data breaches to the appropriate management personnel within the organisation at the earliest possible opportunity, and within 24 hours of the report of the breach.

All actual or suspected data breaches involving personal or health information must be reported to the Institute's Data Breach Assessment Officer.

Where an actual or suspected data breach involves a local or statewide NSW Health system, network or asset (including computer hardware and software), the manager must also report the breach to the Institute's Chief Information Officer.

### 3.4 Data Breach Assessment Officer

The Chief Data Officer will act as the Data Breach Assessment Officer. In the Chief Data Officer's absence, their delegate will act as the Data Breach Assessment Officer.

The Data Breach Assessment Officer supports the CEO in meeting their obligations under the PPIP Act, including the MNDB Scheme, and is responsible for:

- Receiving reports of actual or suspected data breaches involving personal or health information
- Immediately escalating reports of data breaches to the CEO where the data breach is a suspected eligible data breach or where the suspected data breach involves non-personal information that could cause significant harm to the Institute or NSW Health
- Undertaking formal assessment of suspected eligible data breaches under the MNDB Scheme (see section 5.4)
- Following an assessment of a suspected eligible data breach, provide advice to the CEO as to whether the data breach is (or may be) an eligible data breach under the MNDB Scheme
- Ensuring eHealth NSW is notified, where the breach involves unauthorised third-party access to NSW Health systems, networks or assets (including computer software or hardware)
- Identifying and engaging key stakeholders within the organisation to respond to data breaches to ensure all reasonable attempts are made to mitigate the harm done by the suspected breach
- Providing advice to the CEO on whether the matter requires notification, or escalation, to the Ministry of Health

### 3.5 Chief Data Officer

The Chief Data Officer is also responsible for the following:

- Ensure mechanisms are in place to track the status of corrective and preventative actions, breach containment, and provide regular reports to the Data Governance Steering Committee
- Ensure that all Data Breach Incident Management Reports are provided to delegated personnel for review and approval
- Maintain the internal Eligible Data Breach Incident Register for eligible data breaches
- Maintain the Public Notification Register on the Institute's website for eligible data breaches
- The CEO and Chief Data Officer can veto any actions or mitigations in response to a data breach

### 3.6 Chief Information Officer

The Chief Information Officer is responsible for reviewing breaches and:

- Advising on the impact of the breach from technical and security perspectives

- Ensuring containment activities, including shutting down Information Communication and Technology (ICT) systems that are breached, revoking or changing computer access and correcting any weaknesses in physical or technical security are undertaken
- Ensuring technology-related and security corrective and preventive actions are undertaken
- Determining how any associated information security incident be managed and reported as per the NSW Government Cyber Security Policy

### 3.7 Privacy Contact Officer

The Privacy Contact Officer should be notified by the Chief Data Officer of an actual or suspected data breach and is responsible for the following:

- Advise on the impact of a breach from a privacy perspective
- Advise on the corrective and preventive actions and ensure they are appropriate from a privacy perspective
- Participate in consultation and review recommendations following the assessment of an eligible data breach
- Coordinate and prepare notifications to the NSW Privacy Commissioner and/or Ministry of Health for approval of the CEO
- Promote a privacy-aware culture across the organisation

### 3.8 Data Governance Steering Committee

The Data Governance Steering Committee should be notified by the Chief Data Officer of an actual or suspected data breach and is responsible for the following:

- Provide expert advice regarding the breach and any corrective and preventive actions as part of the breach management and containment process
- Review and approve Data Breach Incident Management Reports
- Review the assessment of a suspected eligible data breach and make recommendations to the CEO regarding mandatory notifications
- Coordinate data breach assessment teams, if required
- Advise Strategic Communications and Public Affairs, if required

## 4. What is an Eligible Data Breach?

A data breach occurs when personal information held by the Institute (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.

This may or may not involve disclosure of personal information external to the agency or publicly. For example, unauthorised access to personal information by an agency employee, or

unauthorised sharing of personal information between teams within an agency may amount to a data breach.

A data breach may occur as the result of malicious action, systems failure, or human error.

The MNDB Scheme applies where an 'eligible data breach' has occurred. For a data breach to constitute an 'eligible data breach' under the MNDB Scheme, there are **two tests to be satisfied**:

1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, **and**

2. A reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates.

The term 'serious harm' is not defined in the PPIP Act. Harms that can arise as the result of a data breach are context-specific and will vary based on:

- the type of personal information accessed, disclosed or lost, and whether a combination of types of personal information might lead to increased risk
- the level of sensitivity of the personal information accessed, disclosed or lost
- the amount of time the information was exposed or accessible, including the amount of time information was exposed prior to the agency discovering the breach
- the circumstances of the individuals affected and their vulnerability or susceptibility to harm (that is, if any individuals are at heightened risk of harm or have decreased capacity to protect themselves from harm)
- the circumstances in which the breach occurred, and
- actions taken by the agency to reduce the risk of harm following the breach.

Serious harm occurs where the harm arising from the eligible data breach has, or may, result in a real and substantial detrimental effect to the individual. The effect on the individual must be more than mere irritation, annoyance or inconvenience.

Harm to an individual includes physical harm; economic, financial or material harm; emotional or psychological harm; reputational harm; and other forms of serious harm that a reasonable person in the agency's position would identify as a possible outcome of the data breach.

## 5. Processes for Managing Data Breaches

The Institute must undertake the following steps when responding to a breach:

Step 1: **Initial report and triage** of a data breach

Step 2: **Contain** the breach and do a preliminary assessment

Step 3: **Mitigate** the risk and harm associated with the breach

Step 4: **Assessment** of Data Breaches

Step 5: **Notify** affected individuals and/or others

Step 6: **Prevent** future breaches

The decision on how to respond will be made on a case-by-case basis. Depending on the breach, not all steps may be necessary, or some steps may be combined. In the event of a third-party breach, the Institute will review the relationship with the vendor in line with existing procurement processes.

## 5.1 Step 1: Initial report and triage

All staff members must report any actual or suspected data breach to their manager immediately. Managers at all levels are responsible for escalating reports of actual or suspected data breaches to the appropriate management personnel within the organisation at the earliest possible opportunity and within 24 hours of the report of the breach.

External parties should report incidents directly by email to CINSW-ResearchGovernance@health.nsw.gov.au.

All information regarding any data breach should be documented using the Data Breach Management Incident Report (Internal Reference number E24/07298-1) (**Attachment A**).

The Data Breach Assessment Officer will notify the CEO immediately of a suspected eligible data breach.

The Data Breach Assessment Officer will review the information provided to determine whether it is an eligible data breach under the MNDB Scheme and complete the Internal Data Breach Register.

The CEO may also consider convening a Data Breach Response Team, where a data breach involves highly sensitive information, has a high risk of harm to individuals and affects more than one individual. This will be coordinated by the Data Breach Assessment Officer.

When rapid communication is required outside of standard business hours existing processes for emergency contacts will be called upon.

## 5.2 Step 2: Containment

The Data Breach Assessment Officer will lead the Data and Research Governance Team to take all reasonable steps to contain an actual or suspected data breach.

Where needed, a working group comprising members of the Data Governance Steering Committee will provide additional support and expertise. Containment activities may include:

- Ceasing an unauthorised practice (e.g. the inappropriate collection of data, reporting of data, access of records)
- Recovering or retrieving lost data (e.g., if accidentally left in an inappropriate location, or given to an unauthorised party)

- Suspending activities that led to the breach (e.g. shutting down an ICT system)
- Revoking or changing access codes or passwords

Containment steps are to be taken in consultation and collaboration with relevant subject matter experts, depending on the nature and scope of the data breach.

## 5.3 Step 3: Mitigate risk and harm

Following the initial containment of an actual or suspected data breach, a risk assessment must be conducted by the Data Breach Assessment Officer to identify and undertake mitigation strategies in relation to potential risks arising from the actual or suspected data breach. This must be reported to the Data Governance Steering Committee for further evaluation and discussion.

## 5.4 Step 4: Assessment of Data Breaches

Following receipt of a report of an actual or suspected data breach, the Institute's Data Breach Assessment Officer is to conduct an assessment of the breach.

If the CEO reasonably suspects that the person nominated as the organisation's Data Breach Assessment Officer was involved in an action or omission that led to the breach, the assessment must be undertaken by another staff member determined by the CEO, with the appropriate skills and experience.

### 5.4.1 Determining whether the breach is an eligible data breach

In conducting the assessment, the Data Breach Assessment Officer must determine whether the data breach is considered to be an eligible breach under the MNDB Scheme. The assessment must be conducted with regard to Statutory Guidelines prepared by the NSW Privacy Commissioner on the assessment of data breaches under Part 6A of the PPIP Act.

An Eligible Data Breach Self-Assessment Form should be completed for the CEO's review and approval (E24/07298-2 **Attachment B**).

The Data Governance Steering Committee should provide strategic advice and expertise throughout the assessment and notifications.

### 5.4.2 Assessment period

In conducting an assessment, the Data Breach Assessment Officer must take all reasonable steps to ensure the assessment is completed **within 30 days** after the organisation becomes aware of the breach.

If an assessment cannot reasonably be conducted within 30 days, the CEO may approve an extension for an amount of time reasonably required for the assessment to be conducted. If an extension is granted, the CEO must write to the Privacy Commissioner noting that the assessment has started, that an extension has been approved, and note the period of extension.

If the assessment is not conducted within the extension period, the Chief Executive must, before the end of the extension period, give written notice to the Privacy Commissioner that the

assessment is ongoing, that a new extension period for the assessment has been approved, and provide details of the new extension period.

### 5.4.3 Decision about the data breach

Following the assessment, the Data Breach Assessment Officer must advise the CEO whether the assessment found the data breach to be an eligible data breach, or if there are reasonable grounds to believe the breach is an eligible data breach. The CEO must, on the basis of the assessment, determine whether the data breach is an eligible data breach or that there are reasonable grounds to believe the data breach is an eligible data breach.

## 5.5 Step 5: Notify

While notification to affected individuals is an important mitigation strategy, it will not always be the appropriate response to a breach. Providing notification about low-risk breaches can cause undue anxiety and de-sensitise individuals to future notices. Each incident needs to be considered on a case-by-case basis to determine whether breach notification is required.

### 5.5.1 Immediate notification to Privacy Commissioner

The CEO must immediately notify the Privacy Commissioner of an eligible data breach, using the *Data Breach Notification to the Privacy Commissioner* form available from the NSW Information and Privacy Commission MNDB Scheme webpage (www.ipc.nsw.gov.au/privacy/MNDB-scheme). This notification must also be forwarded to the Ministry of Health at MOH-Privacy@health.nsw.gov.au (E24/07298-3 **Attachment C**).

Where it is not reasonably practicable for the Institute to provide all required information in its original notification to the Privacy Commissioner, the CEO must provide a follow-up notification to the Privacy Commissioner using the same form.

A follow-up notification to the Privacy Commissioner is also to be provided when making a notification to affected individuals, making a public notification of an eligible data breach, or when the CEO determines that an exemption from notifying affected individuals applies.

### 5.5.2 Notifying affected individuals

As soon as practicable after an eligible data breach occurs, the Chief Executive must, to the extent that it is reasonably practicable, take the steps that are reasonable in the circumstances to notify each affected individual of the eligible data breach. Notification to affected individuals should be made in writing and, where it is reasonably practicable for the information to be provided, the notification must include the following:

- the date the breach occurred
- a description of the breach
- how the breach occurred
- the type of breach that occurred
- the personal or health information that was the subject of the breach

- the amount of time the personal or health information was disclosed for
- actions that have been taken or are planned to ensure the personal or health information is secure, or to control or mitigate the harm done to the individual
- recommendations about the steps the individual should take in response to the breach
- information about how to make a privacy complaint to the NSW Privacy Commissioner
- information about how to request a privacy internal review
- if any other NSW Health organisations, or other NSW public sector agencies were the subject of the breach, the name of each organisation and/or agency
- contact details for the organisation or a person nominated by the CEO for the affected individual to contact about the breach

### 5.5.3 Public Notification and Public Notification Register

Where the Institute is unable to notify affected individuals directly, or where it is not reasonably practicable to do so (for example where affected individuals cannot be identified, where the contact information of affected individuals is unknown, or where the volume of affected individuals would cause direct notification to result in an unreasonable diversion of resources), the Institute must publish a public notification on its website and take all reasonable steps to disseminate the notification. This may include publicising the notification via internal or external communication channels depending on the individuals' circumstances of the eligible data breach.

The Institute must also record all public notifications on a publicly available register maintained by the Institute on its website. Details of each public notification are to be published on the publicly available register for at least 12 months from the date the notification is published. The Chief Data Officer is responsible for ensuring the register is kept up to date.

As soon as practicable after a public notification is published, the CEO must, in a follow-up notification to the NSW Privacy Commissioner, provide information about how to access the notification on the publicly available register.

In certain circumstances, the CEO may decide to issue a voluntary public notification in addition to directly notifying affected individuals. This may be appropriate where there has been significant media coverage or interest in connection with a data breach, or where third parties may be significantly impacted by a data breach and public notification would assist in mitigating any harm.

### 5.5.4 Exemption from notifying individuals

If one of the six exemptions set out in Division 4 of the MNDB Scheme applies in relation to an eligible data breach, the Institute may not be required to notify affected individuals. The Information and Privacy Commission (IPC) has produced guidance to agencies on exemptions from notification.

Following a determination by a CEO that an exemption from notifying affected individuals applies, the CEO must provide a follow-up notification to the Privacy Commissioner.

### 5.5.5 Notification to the Ministry of Health

Where an actual or suspected data breach involves a high volume of affected individuals, a risk of adverse media coverage, potential impacts on other NSW Health organisations, or other circumstances that cause the breach to be complex or sensitive, an urgent Incident Brief (using the standard Brief template) must be prepared and submitted to the Ministry of Health by the Privacy Contact Officer.

The Incident Brief must include review by eHealth NSW where the breach involves NSW Health systems or networks, and the NSW Health General Counsel to enable appropriate assessment and, where appropriate, a system-level response.

## 5.6 Step 6: Prevent

Once the immediate steps are taken to mitigate the risks associated with the breach, the Data and Research Governance Team will ensure Corrective and Preventive Actions (CAPAs) are undertaken as part of a strategy of continuous improvement.

Corrective Actions are likely to already have been taken as part of the Contain phase, however additional corrective actions or process changes may be required. Corrective actions must be recorded in the data breach register.

Examples of Preventive Actions (to prevent the breach from re-occurring) may include:

- a security review including a root cause analysis of the data breach
- a prevention plan to prevent similar incidents in the future
- audits to ensure the prevention plan is implemented
- a review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that (for example, security, record retention and collection policies)
- a review of employee selection and training practices
- a review of work practices (e.g., data collection, linking)
- a review of contractual obligations with contracted service providers

Implemented CAPAs must be independently assured by the internal audit and risk function in the Institute, to ensure that agreed actions have been completely, accurately, and effectively applied.

This policy will be reviewed every 2 years by stakeholders in the organization including the Chief Data Officer, Chief Information Officer, Chief Executive Officer, Privacy Officer and relevant divisional directors.

Annual training will be conducted including scenario-based training to ensure that key personnel have extensive exposure to different types of data breaches.

To ensure that executives and key personnel are current with the changing threat landscape and meet expectations of their understanding about this topic, data breaches will be a standing item on the Data Governance Committee meeting and warranted breaches are reported to the Executive Leadership Team which meets on a weekly basis and will be escalated to the board as appropriate.

## 6. Internal Register for Eligible Data Breaches

The Institute must maintain an internal register for eligible data breaches. The internal register is to capture:

- who was notified of the breach
- when the breach was notified
- the type of breach
- details of steps taken by the public sector agency to mitigate harm done by the breach
- details of the actions taken to prevent future breaches
- the estimated cost of the breach, if known

The internal register is maintained using MS Teams and regularly backed up to HPRM or equivalent approved archiving software.

## 7. Additional Reporting Obligations

In addition to the MNDB Scheme, the Institute may be subject to additional mandatory reporting obligations for data breaches affecting certain categories of information, and the following should be considered:

- notification of data breaches involving tax file numbers to the Office of the Australian Information Commissioner (OAIC) under the Privacy Act 1988 (Cth)
- in consultation with eHealth NSW, reporting cyber security incidents to the Australian Cyber Security Centre (ACSC) under the Security of Critical Infrastructure Act 2018 (Cth)
- notification of data breaches involving the My Health Record system to the OAIC and the Australian Digital Health Agency under the My Health Records Act 2012 (Cth)
- notification to the OAIC of any unauthorised recording, use or disclosure of personal information included in the National Cancer Screening Register under the National Cancer Screening Register Act 2016 (Cth)
- reporting to ICAC under section 11 of the Independent Commission Against Corruption Act 1988 where the data breach involves potential corrupt conduct
- notifying law enforcement authorities where the data breach involves criminal conduct

When responding to a data breach, NSW Health organisations must also consider other potential notification obligations not captured above and those arising out of any relevant contractual provisions.

## 8. Glossary

A glossary of terms and definitions is outlined in the table below.

| Term | Definition |
|---|---|
| ASIC | Australian Securities and Investments Commission. |
| CAPA | Corrective and Preventive Actions. |
| CEO | Chief Executive Officer. |
| CDO | Chief Data Officer |
| Data breach | Occurs when personal or health information is lost orsubjected to unauthorised access, modification, disclosure, or other misuse or interference. |
| Data Breach Assessment Officer | A person or persons nominated or appointed by the Chief Executive Officer to assess reports of data breaches involving personal or health information and perform the functions of an assessor under the Mandatory Notification of Data Breach scheme in line with Part 6A, Division 2 of the PPIP Act |
| Eligible data breach | The Mandatory Notification of Data Breach scheme applies where an 'eligible data breach' has occurred.<br>For a data breach to constitute an 'eligible data breach' under the MNDB Scheme there are two tests to be satisfied:<br>1. There is an unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information, and<br>2. A reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates. |
| Eligible data breach incident register | Agencies are required to establish and maintain an internal register of eligible data breaches. This register should record the information specified under section 59ZE(2) of the PPIP Act. |
| Health Information | Health information (within the meaning of the HRIP Act) means:<br>• personal information that is information or an opinion about:<br>  ○ the physical or mental health or a disability (at any time) of an individual, or |

| Term | Definition |
|---|---|
| | ○ an individual's express wishes about the future provision of health services to him or her, or<br>○ a health service provided, or to be provided, to an individual, or<br>• other personal information collected to provide, or in providing, a health service, or<br>• 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, or<br>• 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<br>• healthcare identifiers,<br>Health Information does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information for the purposes of the HRIP Act generally or for the purposes of specified provisions of the HRIP Act. |
| HPP | Health Privacy Principles. |
| HRIP Act | Health Records and Information Privacy Act 2002. |
| ICAC | Independent Commission Against Corruption. |
| ICT | Information Communication and Technology |
| IPC | Information and Privacy Commission |
| ITIL | Information Technology Infrastructure Library |
| Institute | Cancer Institute NSW |
| MNDB | Mandatory Notification of Data Breach scheme |
| NIST | National Institute of Standards and Technology |
| NSW | New South Wales. |
| OAIC | Office of the Australian Information Commissioner |
| PPIP Act | Privacy and Personal Information Protection Act 1998 |
| Personal Information | In the PPIP Act and HRIP Act, personal information means information or an opinion (including information or an opinion forming part of a database and whether recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. |

| Term | Definition |
|---|---|
| | Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.<br><br>Refer to these Acts for what personal information *does not* include (section 5(3) of the HRIP Act). |
| Public Notification Register | Agencies are required to maintain a public notification register of any mandatory notifications made under section 59N(2) of the PPIP Act. The information recorded in the register must be publicly available for at least 12 months after the date of publication and include the information specified under section 59O of the PPIP Act. |
| Serious harm | The PPIP Act does not define serious harm.<br><br>The Information and Privacy Commission guidelines state serious harm can include physical, financial, or material harm, emotional or psychological harm or reputational harm. The impact of the harm can vary from person to person, but may include:<br>• financial loss through fraud<br>• a likely risk of physical or psychological harm, such as by an abusive ex-partner<br>• identity theft, which can affect your finances and/or credit record<br>• serious harm to an individual's reputation.<br><br>In making a determination about the likelihood that a breach would cause serious harm and the consequences and severity of that harm, the agency may consider the following:<br>• the types of personal information involved, for example, an email address is likely to be considered less likely to result in serious harm than credit card details<br>• the sensitivity of the personal information, for example, if it relates to a person's finances, health, or sexual orientation<br>• whether the personal information is or was protected by security measures such as encryption and therefore unlikely to be accessed or misused<br>• who has access to the personal information<br>• whether the person/s who accessed the personal information may have a malicious intent and whether they may be able to circumvent security measures<br>• the nature of the likely harm<br>• any other matter specified in the Privacy Commissioner's guidelines. |

## 9. Attachments

**A.** Data Breach Management Incident Report (Internal reference number E24/07298-1)

**B.** Eligible Data Breach Self-Assessment Form (Internal reference number E24/07298-2)

**C.** Data Breach Notification to the Privacy Commissioner (Internal reference number E24/07298-3)