Data Breaches Involving Personal or Health Information

Summary This policy outlines the minimum requirements and standards across NSW Health 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.

Document type Policy Directive

Document number PD2023_040

Publication date 28 November 2023

Author branch Legal and Regulatory Services

Branch contact (02) 9391 9000

Review date 28 November 2028

Policy manual Not applicable

File number H23/89430

Status Active

Functional group Clinical/Patient Services - Governance and Service Delivery, Information and Data

Applies to Ministry of Health, Public Health Units, Local Health Districts, Board Governed Statutory Health Corporations, Chief Executive Governed Statutory Health Corporations, Specialty Network Governed Statutory Health Corporations, NSW Health Pathology, Public Health System Support Division, Cancer Institute, NSW Ambulance Service, Dental Schools and Clinics, Public Hospitals

Distributed to Ministry of Health, Public Health System, NSW Ambulance Service

Audience All Staff of NSW Health

Secretary, NSW Health

NSW Health

POLICY DIRECTIVE

Data breaches involving personal or health information

POLICY STATEMENT

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

SUMMARY OF POLICY REQUIREMENTS

All staff members have a responsibility to identity and report actual or suspected data breaches to their manager immediately and, where practicable, take appropriate action to contain the breach. When reporting a data breach, staff are encouraged to include as much relevant information as possible.

The Chief Executive of each NSW Health organisation must nominate or appoint at least one appropriately senior staff member as a Data Breach Assessment Officer for their organisation.

All managers 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 NSW Health organisation'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 organisation's Chief Information Officer/Chief Information Security Officer.

Chief executives have ultimate responsibility and accountability for their organisation's response and management of data breaches. This includes making all reasonable attempts to contain data breaches and mitigate any harm done by the breach.

All NSW Health organisations must develop local procedures that enable the organisation to effectively identify and respond to all data breaches that involve personal or health information, including those breaches that require a significant and coordinated effort to contain, mitigate, assess, and manage the response to the breach.

Where an actual or suspected data breach involving personal or health information also involves a high volume of affected individuals, potential impacts on other NSW Health organisations, a risk of adverse media coverage, or other circumstances that cause the breach to be complex or sensitive, an urgent Incident Brief must be prepared and submitted to the Ministry of Health.

Following a report of a data breach involving personal or health information, the organisation's Data Breach Assessment Officer is to conduct an assessment of the breach, including whether the data breach is considered to be an eligible breach under the Mandatory Notification of Data Breach Scheme.

The assessment is to be completed within 30 days after the organisation becomes aware of the breach. The Chief Executive may approve an extension of the assessment period and must notify the Privacy Commissioner any such extension.

The Chief Executive must immediately notify the Privacy Commissioner of an eligible data breach, using the notification form available from the Information and Privacy Commission website www.ipc.nsw.gov.au. This notification must also be forwarded to the Ministry of Health via MOH-Privacy@health.nsw.gov.au.

All NSW Health organisations must maintain an internal register of eligible data breaches that captures set information about each eligible data breach.

As soon as practicable after a Chief Executive determines there are reasonable grounds to believe an eligible data breach has occurred, the NSW Health organisation must, to the extent that it is reasonably practicable, take the steps that are reasonable in the circumstances to notify each affected individual.

If the NSW Health organisation is unable to notify, or if it is not reasonably practicable to notify, any or all of, the affected individuals, the organisation must publish a notification on its website and take reasonable steps to publicise the notification.

All NSW Health organisations must maintain on its website a public register of all public notifications made.

Under certain circumstances, such as where there is an ongoing investigation, where notification would create a serious risk of harm to health or safety, or that notification would compromise the organisation's cyber security, the Chief Executive may determine that the organisation is exempt from notifying individuals of a breach.

Where the Chief Executive determines an exemption is applicable, it must also take into consideration any Statutory Guidelines issued by the Privacy Commissioner in relation to the relevant exemption.

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

REVISION HISTORY

Version	Approved By	Amendment Notes
PD2023_040 November 2023	Secretary	New policy developed outlining obligations following amendments to the *Privacy and Personal Information Protection Act 1998* and the introduction of the Mandatory Notification of Data Breach Scheme.

CONTENTS

1. BACKGROUND

NSW Health holds sensitive information, including personal and health information, about patients, staff and other third parties. All staff members have a responsibility to uphold confidentiality and protect information entrusted to them.

NSW Health organisations are required to have information security measures and controls developed and implemented to ensure privacy of information is preserved, confidentiality of information is protected, integrity of information is maintained, and availability of information is assured. This includes the requirement to have an Information Security Management System (ISMS) or Cyber Security Management System (CSMS) that is compliant with recognised standards and implement the relevant controls based on the organisation's requirements and risk tolerance.

Data breaches can result in serious harm to affected individuals and NSW Health. How NSW Health organisations respond to data breaches impacts the reputation of the NSW Health system, and the degree to which patients, staff and other third parties trust NSW Health with their personal and health information.

Amendments have been made to the *Privacy and Personal Information Protection Act 1998* (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 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.

1.1. Information security and data governance obligations

The *NSW Health Data Governance Framework* (GL2019_002) 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.

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.

1.2. About this document

This Policy Directive outlines the minimum requirements and standards for all NSW Health organisations under the Mandatory Notification of Data Breach Scheme 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 affected individuals.

NSW Health organisations may also be subject to other mandatory notification obligations in relation to the management of data breaches (a non-exhaustive list of additional reporting

obligations is outlined in section 10) when responding to a data breach under this Policy Directive.

NSW Health organisations may adopt this Policy Directive as a local policy supported by procedures tailored for the organisation, or develop their own policy document, provided that the local policy is consistent with the requirements of this Policy Directive and the Mandatory Notification of Data Breach Scheme.

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. Key definitions

Affected individual	A person whose information is subject to a data breach or eligible data breach.
Data breach	Unauthorised access to, disclosure, or loss of any data held by a NSW Heath organisation.
Data Breach Assessment Officer	A person or persons nominated or appointed by the Chief Executive 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	• Unauthorised access to, or unauthorised disclosure of, personal information held by a NSW Health organisation that would be likely to result in **serious harm** to an individual to whom the information relates, or • loss of personal information held by a NSW Health organisation in circumstances where unauthorised access or disclosure is likely to occur, and which would be likely to result in **serious harm** to an individual to whom the information relates. For a data breach to meet the threshold of an eligible data breach, the assessment must establish that a reasonable person would conclude the harm arising from the data breach has, or may, result in a detrimental effect to the affected individual that is more than merely trivial, and there is a real, and not remote, chance of that harm occurring.

held by a NSW Health organisation	For the purposes of the Mandatory Notification of Data Breach Scheme, information is held by a NSW Health organisation where the NSW Health organisation is in possession of the information or the NSW Health organisation has control over the information. This will require an assessment on a case-by-case basis, particularly if there are contractual arrangements in place and the actual or suspected breach involves a third party. Information is also held by a NSW Health organisation where the information is contained in a State record in respect of which the agency is responsible under the *State Records Act 1998*.
NSW Health organisation	A local health district, specialty health network, statutory health corporation, the Ministry of Health, units of the Health Administration Corporation (including the NSW Ambulance Service, HealthShare NSW, eHealth NSW, Health Infrastructure and NSW Health Pathology), and health bodies established under their own statute, including the Cancer Institute of NSW.
Personal information	Refers to information as defined in section 4 of the PPIP Act and, for the purposes of the Mandatory Notification of Data Breach Scheme and this Policy Directive, also includes health information as defined by section 6 of the *Health Records and Information Privacy Act 2002* (see section 11.1-11.2 for further information).
Public sector agency	Refers to organisations as defined by section 3 of the PPIP Act (see section 11.3 for further information).
Staff member	Any person working in a casual, temporary, or permanent capacity in NSW Health, including volunteers, students, consultants and contractors.

1.4. Legal and legislative framework

- *Privacy and Personal Information Protection Act 1998*
- *Health Records and Information Privacy Act 2002*
- *State Records Act 1998*
- *Security of Critical Infrastructure Act 2018*
- *Public Interest Disclosures Act 2022*
- *Data Sharing (Government Sector) Act 2015*
- *Privacy Act 1988 (Cth)*

2. ROLES AND RESPONSIBILITIES

2.1. Responsibilities of staff

All staff members have a responsibility to identity and report actual or suspected data breaches. If a staff member identifies or suspects that a data breach has occurred, they must report the data breach to their manager immediately and, where practicable, take appropriate action to contain the breach.

2.2. Managers

Managers at all levels in each NSW Health organisation 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 NSW Health organisation's Data Breach Assessment Officer.

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

Depending on the type of information involved in the data breach, the data breach may also be reported to the organisation's:

- Information and Records Manager and/or Privacy Contact Officer
- Head of Internal Audit
- Director of Human Resources (where the breach relates to personnel records)
- Director of Clinical Services (where the breach relates to patient records)
- Disclosure Officer (where the report may be a public interest disclosure)
- Data Custodian (where the breach relates to a NSW Health data asset)
- Chief Executive

Where the report arises due to the conduct of another staff member, such as where it is alleged that a staff member has intentionally and inappropriately accessed a person's electronic medical record, the manager must give consideration as to whether the report is a Public Interest Disclosure under the *Public Interest Disclosures Act 2022*.

Further information is available in the NSW Health Policy Directive *Public Interest Disclosures* (PD2023_026).

2.3. Data Breach Assessment Officer

The Chief Executive of a NSW Health organisation must nominate or appoint at least one appropriately senior staff member as a Data Breach Assessment Officer.

The Data Breach Assessment Officer supports the Chief Executive in meeting their obligations under the PPIP Act, including the Mandatory Notification of Data Breach 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 Chief Executive 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 organisation or NSW Health
- Undertaking formal assessment of suspected eligible data breaches under the Mandatory Notification Scheme (see section 6).
- Following an assessment of a suspected eligible data breach, providing advice to the Chief Executive as to whether the data breach is (or may be) an eligible data breach under the Mandatory Notification of Data Breach 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 Chief Executive on whether the matter requires notification, or escalation, to the Ministry of Health
- Preparing notifications to the NSW Privacy Commissioner and/or Ministry of Health for approval of the Chief Executive
- Promoting a privacy-aware culture across the organisation

2.4. Chief executives

Chief executives have ultimate responsibility and accountability for their organisation'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 Mandatory Notification of Data Breach Scheme, the Chief Executive must immediately notify the NSW Privacy Commissioner of the breach.

Following an eligible data breach, the Chief Executive 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.

It is noted that, under the Mandatory Notification of Data Breach Scheme, there are several powers conferred to chief executives. While these powers may be delegated, the Chief Executive must ensure a local decision to delegate powers under the Mandatory Notification of Data Breach 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.

3. ESTABLISHING LOCAL PROCEDURES

All NSW Health organisations must develop local procedures consistent with this Policy Directive that enable the organisation to effectively identify and respond to all data breaches that involve personal or health information, including those breaches that require a significant and coordinated effort to contain, mitigate, assess, and manage the response to the breach.

4. REPORTING A DATA BREACH

4.1. What to include in a report

All staff members must report any actual or suspected data breach to their manager. When reporting a data breach, staff are encouraged to include as much of the information outlined below, as possible:

- the date the breach occurred
- a description of the breach, including whether it is a cyber incident
- how the breach occurred, if known
- who made the breach, e.g. a staff member, threat actor, where known
- the type of breach that occurred, e.g. unauthorised disclosure, unauthorised access, loss of information
- the amount of time the personal or health information was disclosed for
- the personal or health information that was the subject of the breach
- any actions that have been taken to ensure the personal or health information is secure, or to control or mitigate any potential harm done to the individuals who are affected by the breach
- if the breach affects other NSW Health organisations, or other public sector agencies, the details of those organisations and the nature of their involvement or impact on them.

4.2. Protection from detrimental action

Where a staff member is considering reporting a data breach that has occurred due to the conduct of another staff member, such as where it is alleged that a staff member has intentionally and inappropriately accessed a person's electronic medical record, the staff member making the report may also be afforded protection from detrimental action that may arise from making the report.

Further information is available in the NSW Health Policy Directive *Public Interest Disclosures* (PD2023_026).

5. INITIAL RESPONSE TO DATA BREACHES

5.1. Containment

Containing the data breach must be prioritised as part of the data breach response.

Upon becoming aware of an actual or suspected data breach, NSW Health organisations must immediately take all reasonable steps to contain the data breach.

This may include, but is not limited to:

- recovering or retrieving lost data
- suspending activities that led to the breach,
- isolating or suspending affected systems, and/or
- 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 (e.g. Chief Information Officer/Chief Information Security Officer where data breach relates to NSW Health information system, network or computer hardware or software).

5.2. Mitigating risk and harm

The Chief Executive of a NSW Health organisation that has been the subject of an actual or suspected data breach must ensure a risk assessment is carried out to identify and undertake mitigation strategies in relation to potential risks arising from the actual or suspected data breach. Where the circumstances surrounding the actual or suspected breach are unfolding, the risk assessment and mitigation strategies must be regularly reviewed and updated as the matter progresses.

5.3. 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 must be prepared and submitted to the Ministry of Health.

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.

5.3.1. Support in responding to a data breach

Where a NSW Health organisation is unable to effectively respond to a data breach, the matter may be escalated to the Ministry of Health for support and advice.

In escalating to the Ministry of Health, the request must include:

- A clear and concise description of the data breach and its potential impacts on the organisation

- The reason/s for the escalation
- Details of the support needed, or an outline of the requested actions, and a rationale for the support or actions.

Note: Personal or health information that is the subject of the breach must not be forwarded as part of the request for support.

The ownership and management of a data breach, and the costs of resources associated with delivering an appropriate response, remains the responsibility of the NSW Health organisation.

6. ASSESSMENT OF DATA BREACHES

6.1. The Assessor

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

If the Chief Executive 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 Chief Executive, with the appropriate skills and experience.

6.2. 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 Mandatory Notification of Data Breach 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 Assessment Form* is available from the NSW Health intranet page https://internal.health.nsw.gov.au/privacy/.

6.3. Assessment period

In conducting an assessment, the Data Breach Assessment Officer (or other nominated staff member) must take all reasonable steps to ensure the assessment is completed within 30 days after the organisation becomes aware of the breach.

6.3.1. Extension of assessment period

If an assessment cannot reasonably be conducted within 30 days, the Chief Executive may approve an extension for an amount of time reasonably required for the assessment to be conducted.

If an extension is granted, the Chief Executive must write to the Privacy Commissioner noting that the assessment has started, that an extension has been approved, and note the period of extension.

6.3.2. Ongoing assessments

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.

6.4. Decision about the data breach

Following the assessment, the assessor must advise the Chief Executive 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 Chief Executive 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.

7. NOTIFICATION OF ELIGIBLE DATA BREACHES

7.1. Immediate notification to Privacy Commissioner

The Chief Executive 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 Mandatory Notification of Data Breach Scheme webpage at www.ipc.nsw.gov.au/privacy/MNDB-scheme**Error! Hyperlink reference not valid.**. This notification must also be forwarded to the Ministry of Health via MOH-Privacy@health.nsw.gov.au.

Where it is not reasonably practicable for a NSW Health organisation to provide all required information in its original notification to the Privacy Commissioner, the Chief Executive must provide a follow-up notification to the Privacy Commissioner. The follow-up notification must contain any information that was not included in the original notification and must also be provided using the *Data Breach Notification to the Privacy Commissioner* 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 Chief Executive determines that an exemption from notifying affected individuals applies.

7.2. 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 chief executive for the affected individual to contact about the breach.

7.2.1. Public notification

Where a NSW health organisation 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 NSW Health organisation 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.

All public notifications must include the information identified at section 7.2 except to the extent that the information contains personal or health information or information that would prejudice the functions of the NSW Health organisation.

The NSW Health organisation must also record all public notifications on a publicly available register maintained by the NSW Health organisation 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.

As soon as practicable after a public notification is published, the Chief Executive 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, a chief executive 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.

8. EXEMPTION FROM NOTIFYING INDIVIDUALS

If a Chief Executive decides that any of the exemptions from the requirement to notify affected individuals of an eligible data breach applies, the NSW Health organisation may not be required to notify affected individuals.

Following a determination by a chief executive that an exemption from notifying affected individuals applies, the Chief Executive must provide a follow-up notification to the Privacy Commissioner in line with section 7.1 of this Policy Directive.

8.1. Multiple public sector agencies

Where an eligible data breach involves at least one other NSW Health organisation or public sector agency, and each organisation or agency has conducted an assessment of the breach and notified the Privacy Commissioner, the NSW Health organisation is not required to notify affected individuals provided that one of the other NSW Health organisations or public sector agencies involved in the same breach has undertaken to notify affected individuals of the eligible data breach.

8.2. Ongoing investigations and certain proceedings

A NSW Health organisation is not required to notify affected individuals if the Chief Executive reasonably believes notification of the eligible data breach would be likely to prejudice an investigation that could lead to the prosecution of an offence, or proceedings before a court or a tribunal.

8.3. Secrecy provisions

A NSW Health organisation is not required to notify affected individuals where compliance with notification requirements would be inconsistent with a provision of an Act or statutory rule that prohibits or regulates the use or disclosure of information.

For example, if the eligible data breach involved information relating to a mandatory report under the *Children and Young Persons (Care and Protection) Act 1998* or a serious adverse event review under the *Health Administration Act 1982*. Advice can be sought from Legal Unit via nswh-legalmail@health.nsw.gov.au in relation to the application of this exemption.

8.4. Successful harm mitigation

In circumstances where an eligible data breach involves unauthorised access to, or disclosure of personal or health information, a NSW Health organisation is not required to notify affected individuals provided that the organisation has already taken action to mitigate harm done by the breach and:

- the action is taken before the breach results in serious harm to an individual, and
- because of the action taken, a reasonable person would conclude that the breach would not be likely to result in serious harm to the individual.

If the eligible data breach involves a loss of personal or health information, a NSW Health organisation is not required to notify affected individuals where the organisation has taken action to mitigate the loss and:

- the action is taken before there is any unauthorised access or disclosure to the information, and
- because of the action taken no unauthorised access to or disclosure of the information occurs.

8.5. Serious risk of harm to health and safety

Where a Chief Executive reasonably believes notification would create a serious risk of harm to an individual's health or safety, the NSW Health organisation is not required to notify those individuals. This exemption is likely to only apply in exceptional circumstances based on the nature and context of the breach and the unique characteristics and circumstances of the affected individual.

In determining whether to rely on this exemption, the Chief Executive:

- must have regard to the Statutory Guidelines prepared by the Privacy Commissioner on the exemption for risk of serious harm to health or safety under section 59W of the PPIP Act, and
- must consider the extent to which the harm of notifying the breach is greater than the harm of not notifying the breach, and
- must consider the currency of the information relied on in assessing the serious risk of harm to an individual, and
- must not search data held by the agency, or require or permit the search of data held by the agency, that was not affected by the breach, to assess the impact of notification unless the Chief Executive knows, or reasonably believes, there is information in the data relevant to whether this exemption applies.

Where a Chief Executive makes such a decision not to notify, they must notify the Privacy Commissioner that the exemption under section 59W is relied on, confirm whether the exemption is permanent or temporary, and, if the exemption is temporary, of the specified or expected time the exemption is to be relied on.

8.6. Compromised cyber security

In determining whether to rely on this exemption, the Chief Executive must first seek guidance from eHealth NSW and have regard to the Statutory Guidelines prepared by the Privacy Commissioner on the exemption for compromised cyber security under section 59X of the PPIP Act.

Following advice from NSW Health's Chief Information Security Officer, where a Chief Executive reasonably believes notification would either worsen the organisation's cyber security, or lead to further data breaches, the NSW Health organisation is not required to notify affected individuals, for the period of time that the Chief Executive reasonably believes this impact is likely.

Reliance on this exemption must be temporary and reviewed monthly. Where this exemption is relied upon, written notice must be provided to the Privacy Commissioner advising that the exemption is relied on, confirming when the exemption is expected to end, and including details of the method the organisation will use to review the exemption.

The Privacy Commissioner is to be provided with an update upon each monthly review of the exemption.

9. INTERNAL REGISTER FOR DATA BREACHES

All NSW Health organisations 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.

10. ADDITIONAL REPORTING OBLIGATIONS

In addition to the Mandatory Notification of Data Breach Scheme, NSW Health organisations may be subject to additional mandatory reporting obligations for data breaches affecting certain categories of information.

NSW Health organisations must also consider:

- 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.

11. APPENDICES

11.1. Definition of personal information

Under section 4 of the PPIP Act, personal information means information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Personal information includes such things as an individual's fingerprints, retina prints, body samples or genetic characteristics.

Personal information **does not** include any of the following:

- information about an individual who has been dead for more than 30 years,
- information about an individual that is contained in a publicly available publication,
- information about a witness who is included in a witness protection program under the *Witness Protection Act 1995* or who is subject to other witness protection arrangements made under an Act,
- information about an individual arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* of the Commonwealth,
- information about an individual that is contained in a public interest disclosure within the meaning of the *Public Interest Disclosures Act 2022,* or that has been collected while dealing with a voluntary public interest disclosure in accordance with that Act, Part 5, Division 2,
- information about an individual arising out of, or in connection with, an authorised operation within the meaning of the *Law Enforcement (Controlled Operations) Act 1997,*
- information about an individual arising out of a Royal Commission or Special Commission of Inquiry,
- information about an individual arising out of a complaint made under Part 8A of the *Police Act 1990,*
- information about an individual that is contained in Cabinet information or Executive Council information under the *Government Information (Public Access) Act 2009*,
- information or an opinion about an individual's suitability for appointment or employment as a public sector official,
- information about an individual that is obtained about an individual under Chapter 8 (Adoption information) of the *Adoption Act 2000*,
- information about an individual that is of a class, or is contained in a document of a class, prescribed by the regulations for the purposes of this subsection.

For the purposes of this Act, personal information is ***held*** by a public sector agency if—

- the agency is in possession or control of the information, or

- the information is in the possession or control of a person employed or engaged by the agency in the course of such employment or engagement, or
- the information is contained in a State record in respect of which the agency is responsible under the *State Records Act 1998*.

For the purposes of the PPIP Act, personal information is not ***collected*** by a public sector agency if the receipt of the information by the agency is unsolicited.

11.2. Definition of health information

Under section 6 of the *Health Records and Information Privacy Act 2002*, health information means:

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

It **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.

11.3. Definition of a public sector agency

A public sector agency means any of the following:

- a Public Service agency or the Teaching Service,
- the office of a political office holder within the meaning of the *Members of Parliament Staff Act 2013*, being the office comprising the persons employed by the political office holder under Part 2 of that Act,
- a statutory body representing the Crown,
- an auditable entity within the meaning of the *Government Sector Audit Act 1983* or any other entity within the meaning of that Act (or entity of a kind) prescribed by the regulations, but excluding an entity (or entity of a kind) prescribed by the regulations,

- the NSW Police Force,
- a local government authority,
- a person or body that:
    - provides data services (being services relating to the collection, processing, disclosure or use of personal information or that provide for access to such information) for or on behalf of a body referred to above, in this definition, or that receives funding from any such body in connection with providing data services, and
    - is prescribed by the regulations for the purposes of this definition.