CHQ Data Breach Policy

Children's Health Queensland Hospital and Health Service (CHQ) is committed to handling your personal information with care, and in accordance with privacy law. CHQ complies with the Queensland *Information Privacy Act 2009* (Qld) (IP Act) and the privacy principles under that Act (known as the Queensland Privacy Principles (QPPs)).

The purpose of this Data Breach Policy is to provide oversight to our consumers on the process for escalating and managing a data breach, including an eligible data breach, at CHQ in order to meet CHQ's statutory obligations under the Mandatory Notification of Data breach scheme (MNDB scheme) in Chapter 3A of the IP Act.

This CHQ Data Breach Policy should be read in conjunction with CHQ Privacy Policy.

Data Breach

A data breach is the unauthorised access to, unauthorised disclosure of, information held by CHQ, or the loss of information held by CHQ in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.

Some examples of data breaches include:

- Phishing emails which trick a user into performing an action or providing information.
- An email is sent to the wrong recipient.
- File is left in a public place.
- Lost or stolen laptops, removeable storage devices, or physical files containing personal information.
- A staff member accessing a patient record without having a valid work reason for doing so.

Eligible Data Breach

Under the MNDB scheme, CHQ has a number of obligations in respect of certain data breaches of personal information ('eligible data breaches'), including notifying the Information Commissioner and affected individuals in the event of an eligible data breach.

A data breach is an eligible data breach when both of the following apply:

- There is unauthorised access to, or unauthorised disclosure of, personal information held by CHQ, or there is a loss of personal information held by CHQ in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
- The unauthorised access to, or disclosure of the information is likely to result in serious harm to an individual to whom the information relates.

The harm that potentially arises from a data breach will vary depending on the nature of the personal information and the context of the data breach.

Serious harm may include:

- Physical, psychological, emotional, or financial harm to the individual because of the access or disclosure.
- Harm to the individual's reputation because of the access or disclosure.

Roles and Responsibilities

CHQ's Privacy and Confidentiality Contact Officer leads the CHQ response, investigation and assessment of any actual or suspected data breach and works closely with relevant internal and external stakeholders such as technical and information security teams to form a Data Breach Response Team as part of any response to a data breach.

Role	Responsibility
Privacy and Confidentiality Contact Officer (**PCCO**)	• Preliminarily assessment of the actual or suspected Data breach. • Internal escalation of data breaches, as required. • Manage and coordinate the Data Breach Response Team. • Notify the Information Commissioner, affected persons and others where required of an eligible data breach. • Comply with record keeping obligations. • Maintain and update the consumer policy (this policy).
Patient Experience Team	• Escalate any actual or suspected data breach reported by a patient or family member to the PCCO.
Data Breach Response Team	• Assess whether a data breach is an eligible data breach, the severity of a data breach. • Consider whether to notify cyber security group agencies where appropriate. • Escalate the appropriate and necessary containment measures and root cause eradication where the data breach is a system related breach. • Conduct post-breach review.
CHQ Employee	• Understand the Data Breach Policy and governance requirements. • Protect personal information under the IP Act from unauthorised access, disclosure, or loss. • Report suspected or confirmed breaches immediately to the appropriate office
Line Manager	• Ensure staff complete mandatory cybersecurity and privacy training and understand relevant policies. • Contain data breaches through appropriate measures. • Report breaches, suspected breaches, and policy violations promptly to the PCCO.

Reporting a Data Breach

Preparation

CHQ has established controls, systems and processes to effectively identify and manage data breaches. Technological measures such as advanced monitoring tools for real-time detection are utilised to ensure prevention and early identification of data breaches.

CHQ also has detailed internal response procedures which sets out the detailed processes for response to any actual or suspected data breach.

CHQ provides appropriate training to staff in identifying, responding to, and managing data breaches.

Internally reported data breach

If a CHQ staff member identifies a potential data breach, they are required to adhere to internal CHQ procedures and:

- Complete the online reporting form, or
- Contact the PCCO directly (only if requiring assistance).

Externally reported data breach

External agencies or members of the public may identify a potential data breach that has occurred within CHQ. These agencies and members of the public are encouraged to contact CHQ immediately upon identification to ensure timely investigation and management by emailing chq_phainfoprivacy@health.qld.gov.au.

Patients or their family can also contact the CHQ Patient Experience team on phone 3068 1120 or by emailing CHQ_PatientExperience@health.qld.gov.au to express concerns or report a suspicion of inappropriate access to patient information by a CHQ staff member.

On reporting to the Patient Experience Team, the team member is required to:

- Complete the online reporting form, or
- Contact the PCCO directly (if requiring assistance).

Containment and Mitigation

All reasonable steps will be taken to contain the data breach. This obligation to contain and mitigate any harm arising from the data breach is ongoing. The containment measures will depend on the nature of the data breach and may include:

- Making efforts to recover and/or destroy the personal information.
- Securing, restricting access to, or shutting down breached systems in consultation with the Digital Health Service.
- Suspending the activity that led to the data breach.
- Revoking or changing access codes or passwords.

All reasonable steps will be taken to contain the breach and take appropriate actions to reduce the risk of serious harm for affected individuals.

Initial Evaluation

Once a data breach (or suspected data breach) has been reported, the PCCO will ensure that it is recorded within CHQ's Data Breach Register to support tracking the status of the breach and compliance reporting.

The PCCO will initially assess the data breach.

Prioritising a data breach will differ on a case-by-case basis and will depend on:

- The sensitivity of the information and circumstances.
- Who was the information disclosed to.
- What happened to the information once it was disclosed.
- How the information was disclosed; and
- If there was any misconduct involved.

Breach priority may change based on further investigation outcomes.

Timeframe

An actual or suspected data breach must be investigated and managed as soon as CHQ is aware of the data breach, or suspects that it has occurred. CHQ must take all reasonable steps to complete an assessment within 30 calendar days after the day CHQ becomes aware of the grounds to suspect the data breach but is not yet certain that it is an eligible data breach.

If CHQ is satisfied that it will be unable to complete the assessment in 30 days, it can extend that time under section 49 of the IP Act.

External Entity Engagement

Effective data breach management requires coordinated action with key external entities, including third-party vendors, law enforcement, and external cybersecurity experts. When a breach occurs, the Data Breach Response Team will engage relevant stakeholders based on the breach's scope and severity.

Third-Party Vendors: Assess potential involvement in the breach, ensure contractual compliance, and coordinate remedial actions.

Law Enforcement: Engage authorities when breaches involve criminal activity, fraud, or legal violations.

External Cybersecurity & Legal Experts: Seek specialised expertise for forensic investigations, compliance guidance, and risk mitigation.

Proactive collaboration strengthens response efforts, ensuring swift containment, compliance adherence, and protection of affected individuals.

Eligible Data Breach

The PCCO will be responsible for conducting a preliminary assessment of any actual or suspected eligible data breach. The PCCO will be the lead contact for all aspects of the initial assessment and investigation.

The preliminary assessment will consider the following:

- Is the personal information likely to have been lost, disclosed, or accessed?
- What type and volume of personal information does the breach involve?
- What types of individuals and how many are or may be affected by the breach (take note if they are a particularly vulnerable demographic)?
- What was the cause of the breach and is a supplier involved?
- What is the extent of the breach, including the period of the breach?
- If the breach was caused by third party interference (hacking), what are the possible motives behind the breach, and is malicious use of the information a possibility?
- What are the possible harms that may occur to individuals affected by the breach?
- How serious is the harm and is that potentially serious harm likely to occur to anyone?
- How can the breach be contained and remediated and if lost, secured or recovered so that an exception applies (remedial action in relation to the access, disclosure, loss) including confirmation is encrypted and encryption key is safe?
- Is the information subject to the actual or suspected access, loss or disclosure stored by an international database?
- An initial view as to whether notification is likely to be required under the IP Act.

If the preliminary assessment deems an actual or suspected data breach is an eligible data breach, the PCCO will convene a meeting of the Data Breach Response Team within 24 hours of completing the preliminary assessment.

The Data Breach Response Team may comprise of the following team members:

- The PCCO
- A CHQ Legal Officer
- A Health Information Access (HIA) Team Officer
- A Human Resources team member
- Manager, Data Services.

The PCCO may also include additional team members in the Data Breach Response Team, depending on the nature of the data breach, such as:

- Director, Health Information Service

- An Information Security team member
- Senior Director, Digital Health Service
- Executive Member
- Director, IT Operations
- Manager, Service Delivery.

Upon completion of the assessment, the Data Breach Response Team must make a recommendation to CHQ Director Health Information Service as to whether:

- The data breach is likely to result in serious harm to the Affected Individual or individuals.
- Mandatory notification to the Information Commissioner and Affected Individuals is required.
- An exemption applies.
- If notification is not mandatory, whether voluntary notification to the Information Commissioner, Information Commissioner and/or Affected Individuals is desirable, in light of applicable data security obligations.

The Data Breach Response Team should also consider whether any other organisations, individuals or entities should be made aware of the data breach such as:

- Third party service providers.
- Regulators.
- Insurers.
- law enforcement authorities.
- Cybercrime support networks (the Australian Cybercrime Online Reporting Network and the Computer Emergency Response Team).

Notification

If the Data Breach Response Team forms the view that the eligible data breach is likely to result in serious harm to the affected individual or individuals, and that recommendation has been approved by the Director Health Information Service, then CHQ will notify the Information Commissioner and affected individuals in the prescribed from, unless an exemption applies.

Exemptions

Section 55 to 60 of the IP Act provides exemptions to the mandatory notification of eligible data breaches. Exemptions to notification obligations exist when:

- Notification would be likely to prejudice an investigation that could lead to the prosecution of an offence or proceedings before a court or tribunal.
- All of the personal information the subject of the data breach is the subject of the data breach of another agency, the other agency has undertaken to conduct the assessment in relation to the data breach and the other agency is required to comply with the notification obligations in relation to the data breach.
- CHQ has taken remediation action to sufficiently mitigate the harm caused by the data breach before there is unauthorised access or disclosure or before that access or disclosure causes serious harm to any individual.
- CHQ’s compliance with the obligation to notify would be inconsistent with a provision of an Act of the Commonwealth or a State that prohibits or regulates the use or disclosure of information. The ICT Incident Response Team should obtain CHQ's Legal's advice as to the application of this exemption.
- CHQ’s compliance with the obligation to notify would create a serious risk of harm to an individual's health or safety, and the harm caused is greater than the harm of not complying with that division. The ICT Incident Response Team should document the risk of harm.
- CHQ’s compliance with the obligation to notify would compromise or worsen CHQ’s cybersecurity or lead to further data breaches of the agency. The ICT Incident Response Team should seek expert opinion as to the application of this ground.

Notification to the Information Commissioner

the Data Breach Response Team will prepare a Notification Statement and provide it to the Information Commissioner as soon as practicable after forming the belief that there has been an eligible data breach.

Where notification is not mandatory, but the ICT Incident Response Team forms the view that the voluntary notification is warranted, the Data Breach Response Team may prepare a Notification Statement and provide it to the Information Commissioner.

Notification to Affected Individuals

Individuals/organisations affected by an eligible data breach will be notified (whether directly or indirectly) as soon as practicable. However, CHQ will need to ensure it has sufficient information about the data breach before issuing notifications.

Wherever possible, notification will be made to all affected individuals. If that is not practicable, CHQ will publish a notice on its website, at Children's Health Queensland, and take reasonable steps to publicise the statement, such as:

- Taking out an advert in the local newspaper.
- Making an announcement on the local radio station.
- Posting a notice on any social media accounts CHQ holds.

The ICT Incident Response Team will keep a record of:

- The date, time, and method of notification to each individual.
- Any confirmation of receipt of the notification received from an individual (unless the data breach involves a very large number of individuals, and it would be impractical to do so).

Post-Data-Breach Review and Remediation

Once all actions related to the eligible data breach or suspected eligible data breach have been addressed, the PCCO will update the data breach register, recording:

- A description of the data breach.
- If submitted, the Notification Statement.
- If applicable, further information requested by the Information Commissioner.
- If applicable, the exemption relied on.
- Details of steps taken to contain or mitigate the eligible data breach.
- Details of steps taken to prevent future data breach of a similar kind occurring.

Either the PCCO or the Data Breach Response Team (if one had been activated) must document the process of any remedial action and ensure there is a record of the rationale and reasoning behind each conclusion.

If applicable, CHQ will update the Risk Register or other internal risk assessment tools.

If the data breach required CHQ to notify the Information Commissioner, after a response is received, the ICT Incident Response Team or an appropriate independent investigator will conduct an assessment on how:

- CHQ responded to the data breach.
- The effectiveness of the supporting governance documentation.
- Provide a recommendation on any changes to processes or procedures that are required to proactively manage future data breaches.

Each quarter the PCCO will supply the CHQ Compliance and Governance team with a de-identified report of all incidents of potential inappropriate access for compliance reporting to the CHQ Audit and Risk Committee.

Prevention Strategies

The IP Act requires CHQ to take proactive steps to contain, assess and mitigate data breaches. The PCCO will leverage the data compiled in the Data Breach Register to identify trends and implement preventive measures against recurring data breaches.

Data Breach Plan reviews

Automatically reviews after a data breach in the post data breach review. Reviews in relation to any major change to legislation etc. and review incorporated with CHQ annual incident response exercises.

Record Keeping and Evidence Preservation

The PCCO is responsible for:

- Preserving any relevant evidence and records/information relating to the breach or investigation process, including breaches that do not get escalated to the Data Breach Response Team or do not meet the eligible data breach threshold; and
- Keeping and recording all information required to the Data Breach Register.

Records are kept of all steps taken in response to the data breach or and any other decisions made in connection with it. CHQ maintains a Data Breach Register, in which all steps taken with respect to the actual or suspected data breach are recorded.

Relevant evidence is stored securely, quarantined, and recorded.

Changes to our Data Breach Policy

We may update our Data Breach Policy as needed to reflect changes in our practices or obligations under the law. When we make changes, we'll post the revised Policy on our website with a new effective date. We encourage you to check for updates periodically.

Additional information and resources

Information and resources for the community and CHQHHS employees are available across a wide variety of privacy-related topics and can be accessed via the links below (note: some of these links will direct you to websites outside of CHQHHS:

- Information Privacy Act 2009 - Queensland Legislation - Queensland Government
- Basic Guide to the Queensland Privacy Principles
- Health agencies – Privacy, confidentiality, and children's information | Office of the Information Commissioner Queensland

Appendix 1 - Definitions

Term	Meaning
Affected individual	In relation to a data breach, an 'affected individual' under section 47(1)(a)(ii) or (b)(ii)of the IP Act.
Data breach	In relation to information held by CHQ: a. unauthorised access to, or unauthorised disclosure of, the information; or

	b. the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur.
Data Breach Policy	This policy.
Data Breach Register	SharePoint register used by the PCCO and HIA personal to track and report on actual and suspected Data breaches within CHQ
Data Breach Response Plan	A more detailed procedural document complementing the Data Breach Policy, which could be an internal document detailing CHQ's more specific processes in managing and responding to a data breach.
Eligible data breach	A data breach of CHQ in relation to personal information held by CHQ if: d. there has been unauthorised access to, or unauthorised disclosure of personal information held by an agency, or e. loss of personal information held by an agency that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, and f. (c) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.
Information Commissioner	The Queensland Information Commissioner
IP Act	The *Information Privacy Act 2009* (Qld)
Held or hold in relation to personal information	Personal information is held by a relevant agency, or the agency holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant agency.
Notification Statement	A notification statement for a privacy breach is a formal communication issued to affected individuals and relevant authorities, informing them of a data breach involving personal information.
Personal information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: c. whether the information or opinion is true or not, and b. whether the information or opinion is recorded in a material form or not.
Serious harm	To an individual in relation to the unauthorised access or unauthorised disclosure of the individual's personal information, includes, for example: a. serious physical, psychological, emotional or financial harm to the individual because of the access or disclosure, or b. serious harm to the individual's reputation because of the access or disclosure.