Central Queensland Hospital and Health Service

Great care for Central Queenslanders

CQHHS Data Breach Policy

Version: 1.0

Publish date: July 2025

Review date: June 2026

Queensland Government

Revision and approval history

Document Executive		Chief Finance Officer, Assets and Commercial Services			
Document Steward		Information Governance Committee			
Risk Rating		Medium 12			
Approval Authority		Information Governance Committee			
Keywords		Data, Eligible Data Breach, Breach Response, MNDB, Mandatory Notification, Privacy, Personal, Sensitive, Information, QPP			
Supersedes		New Policy			
Version	**Approved**	**Effective**	**Authority**	**Comment**	**Review**
1.0	27/06/2025	1/07/2025	Chief Finance Officer	NA	30/06/2026

For more information contact:
CQHHS Privacy and Confidentiality
Central Queensland Hospital and Health Service, Rockhampton Hospital
Canning Street, ROCKHAMPTON QLD 4700

Email: cqhhs-privacy@health.qld.gov.au

Contents

Purpose and scope 4
Definitions 4
Responding to a data breach 5
Identifying a data Breach 5
Containment and mitigation 6
Assessment 6
Notification 7
Notification of affected individuals 7
Notification to other affected agency or organisation 7
Notifying other entities 7
Public Interest Disclosures 8
Exemptions to Notify 8
Notification Strategy 8
Public Notification 8
Post data breach review and evaluation 9
Register of eligible data breaches 9
Record Keeping 9
Related Legislation and Standards 9

Purpose and scope

This Data Breach Policy (**Policy**) sets out how the Central Queensland Hospital and Health Service will respond to data breaches involving personal information including the detection of, responding to, managing notifications, and reporting eligible data breaches in accordance with the Mandatory Notification of Data Breach Scheme (**the MNDB Scheme**) under Chapter 3A of the *Information Privacy Act 2009* (QLD) (IP **Act**).

The MNDB scheme requires the publication of a Data Breach Policy.

This Policy applies to and must be adhered to and implemented by all employees, volunteers, students, and consultants, visiting medical officers and health professionals, contractors, vendors and contracted service providers, within CQHHS.

Staff should consult internal procedures for detailed guidance on how to respond to a data breach in accordance with this Policy.

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 the Central Queensland Hospital and Health Service
Data Breach Response Team	is a team consisting of senior CQHHS personnel responsible for coordinating and managing an eligible data breach.
Eligible Data Breach	*Always* involves personal information and involves an actual or potential loss of, unauthorised access to, or unauthorised disclosure of personal information, which is “likely to result in serious harm” to one person or more.
Ineligible data breach	A data breach that does not meet the criteria to be considered "notifiable" under the Mandatory Notification of Data Breaches (NDB) scheme. This means the breach doesn't require notification to the affected individuals.
Personal Information (s.42 IP Act)	Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion— (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.
Suspected Eligible data breach	Information supports a reasonable suspicion that it is more than possible the breach is an eligible data breach and requires further assessment.
Staff	Any person working in a casual, temporary, or permanent capacity in the CQHHS, including volunteers, students, consultants, and contractors.

Responding to a data breach

The CQHHS takes reasonable security safeguards against the loss, unauthorised access, use, modification and disclosure of personal information, including system wide preventative measures such as

- strong access controls,
- unique usernames and complex passwords,
- data encryption, and
- continuous system and network monitoring,

As well as local measures that assist staff in proactively preventing data breaches from occurring through best practice information management processes, such as:

- limiting physical access to areas where physical records are stored,
- providing staff training and
- providing clear policies and procedures
- data breach clauses included in contracts with external service providers.

Identifying a data Breach

A data breach occurs when there has been unauthorised access to, unauthorised disclosure of, or loss of personal information held by the CQHHS, or any accidental or unlawful destruction or alteration of personal information held by the CQHHS.

A data breach may occur as the result of a malicious action, systems failure, or human error. A data breach may occur also because of misunderstanding as to whether a particular act or practice is permitted under the *Information Privacy Act* 2009 or the *Hospital and Health Boards Act 2011*.

Examples of a data breach include:

Malicious or criminal attack

- Cyber incidents such as ransomware, malware, hacking, phishing or brute force access attempts resulting in access to or theft of personal information.
- Use of deception or impersonation leading into inappropriate disclosure of personal information.
- CQHHS employees using their valid credentials to access or disclose personal information outside the scope of their duties or permissions.
- Theft of a physical asset such as a paper record, laptop, USB stick or mobile phone containing personal information.

System Fault

- Where systems are not maintained through the application of known and supported patches.
- Where a coding error allows access to a system without authentication, or results in automatically generated notices including the wrong information or being sent to incorrect recipients.

Human Error

- personal information is emailed or posted to the wrong recipient.

- Forwarding an email to the wrong distribution list, not using appropriate encryption software or an approved secure file transfer service.
- a portable device or physical record containing personal information is lost or misplaced.
- staff failing to implement appropriate password and system security, by not securing passwords or sharing their password and log in information with other staff.
- When system access is incorrectly granted to someone without appropriate authorisation.
- Staff misusing their legitimate access to browse personal information of a consumer without a legitimate reason.

Members of the public who identify or become aware of a possible data breach potentially involving the CQHHS, should make a report to the CQHHS Consumer Feedback Team as soon as practicable.

Containment and mitigation

The CQHHS recognises that data breaches require immediate and effective response. Containing the data breach must be prioritised as part of the data breach response plan.

Any staff member who has identified or receives information about an actual or suspected data breach must take immediate steps to contain and reduce the impact of the data breach, and to stop further harm. 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

The Information Governance Committee (IGC) holds overarching responsibility for the management and response to data breaches. Where the IGC forms the sufficient belief that the data breach has the potential to likely cause harm to any individual, the IGC will stand up the Data Breach response Team who will carry out a comprehensive assessment of the data breach in accordance with the Data Breach Response Plan.

The Data Breach Response Team will include:

- Chief Finance Officer (IGC Chair)
- Director Information Technology
- ICT Governance, Risk and Compliance Officer
- Director Corporate Governance
- Nurse Manager Clinical Informatics
- Manager Human Resource Services
- Practice Leader Clinical Audit and Quality Improvement
- Communications Representative

Assessment

Where the data breach is a suspected eligible data breach that requires further investigation, the Information Governance Committee (IGC) Chair will conduct an assessment within 30 days of the initial report, to confirm whether the data breach meets the requirements of an eligible data breach under the MNDB Scheme.

If an extension of the assessment period is required, in accordance with section 49 of the IP Act, the CQHHS will give written notice to the Information Commissioner that the assessment will not be completed within the prescribed time.

Notification

If a data breach is determined to be an eligible data breach, the IGC Chair will:

- immediately notify the Queensland Information Commissioner in accordance with Section 51 (2) of the IP Act.
- as soon as possible and in accordance with section 53 of the IP Act, notify affected individuals (unless an exemption is applied in line with Chapter 3A, part 3, division 3 of the IP Act).

The IGC Chair may elect to make a voluntary notification of a data breach to the Information Commissioner, even if the breach is not an eligible data breach.

The CQHHS recognises the importance of notifying individuals / organisations affected by a data breach as soon as practicable. To avoid unnecessary harm, panic, and concern, notifications will not occur prior to the CQHHS ensuring sufficient information is known about the breach.

Individual or public notifications will not occur prior to receiving approval from the Chief Finance Officer.

Notification of affected individuals

In accordance with section 53 of the IP Act, if it is reasonably practicable to notify each affected individual, the CQHHS will take reasonable steps to notify each affected individual directly and inform the affected individuals of their right to lodge a privacy complaint. This may be done by telephone, letter, email or in person.

Where the CQHHS is unable to notify all affected individuals, in accordance with section 53(1)(c), a public notification will be published on our website.

Notification to other affected agency or organisation

Where data from another agency or organisation is involved in the data breach, at the direction of the IGC Chair, the Data Breach Response Team will inform the other agency of the data breach and consult with the relevant party regarding the responsibilities and any further steps needed to respond to the breach.

Notifying other entities

The CQHHS may engage with and notify other entities in response to a data breach where appropriate on a case-by-case basis. This may include but is not limited to:

- Crime and Corruption Commission Queensland
- Queensland Government Information Security Virtual Response Team
- Queensland State Archivist (e.g. Loss or destruction of public records)
- QLD Police
- QG Insurance Fund
- Office of the Australian Information Commissioner (e.g. Tax File Number recipients)

Public Interest Disclosures

Data breaches identified as part of a public interest disclosure must also be managed in accordance with the *Public Interest Disclosure Act 2010.*

Exemptions to Notify

Prior to notifying affected individuals the IGC will have consideration for the notification exemptions outlined in section 55 to 60 of the IP Act. The CQHHS recognises that the notification exemptions are intended to apply only in exceptional circumstances.

Where an exemption to notification must be applied to a data breach, the CQHHS will notify the Information Commissioner in writing that the CQHHS is exempt from complying with the notification obligations outlined in the MNDB Scheme.

Notification Strategy

To meet the requirements of the MNDB Scheme, and support the data breach response plan, the Information Governance Committee will develop a data breach notification strategy to identify specific roles, responsibilities, and communications in the event of an eligible data breach. The strategy must outline:

- who is responsible for communications and other key contacts for communications activities
- a timeline for when affected individuals or organisations will be notified
- how affected individuals will be contacted and managed
- a template of requirements for eligible data breach communications (data breach communications response template), and
- responsibilities for consulting with external stakeholders.

Public Notification

Where appropriate, in accordance with 53(1)(c) of the IP Act, if the CQHHS is unable to contact individuals, the CQHHS must publish a notice of the data breach on our website for a least 12 months and advise the Information Commissioner how to access the notice.

A data breach public notice will include specific details as outlined in section 53(2) of the IP Act, to the extent it is reasonably practicable. Information that may prejudice our functions as a health agency will not be published in the notice.

The public notice will include:

- our name and the name of any other agency affected by the data breach.
- contact details for where an affected individual can contact us in relation to the data breach
- the date the data breach occurred (if known)
- a description of the data breach and how the data breach occurred
- what steps an affected individual should take in response to the data breach
- how we contained the data breach and mitigated the harm caused to affected individuals
- information about how an individual can make a privacy complaint

Post data breach review and evaluation

The Data Breach Response Team where established, must conduct a post-breach review and evaluation to:

- identify weaknesses in the processes, systems or activities that may have contributed to the breach
- assess the effectiveness of data breach response activities under this policy
- develop a proposed action plan of preventative measures and mitigation strategies to be put in place for each identified weakness for the approval by the IGC Chair.
- propose relevant updates to the guiding policies and procedures.
- assess the capability, expertise and resourcing of the data breach response team

Register of eligible data breaches

Section 72 of the IP Act requires the CQHHS to maintain an internal register of eligible data breaches.

The Information Governance Committee will be responsible for maintaining the Internal Data Breach Register recording all instances of eligible and ineligible data breaches, including as a minimum:

- a description of the data breach,
- the steps taken by the CQHHS to contain and mitigate the breach and its harm.
- actions taken by the CQHHS to prevent future data breaches of a similar kind occurring.
- whether the breach is an eligible data breach under section 47

Where the breach is an eligible data breach, the register must also include:

- the date the CQHHS gave a statement to the Information Commissioner about the eligible data breach and the date any additional information was provided to the Commissioner.
- if individuals were directly notified about the eligible data breach, the names of individuals who were notified, the date they were notified, and the method by which they were notified.
- if an exemption was relied on exempting notification to either the Information Commissioner or individuals, and the details of the exemption.

Record Keeping

Any records created in response to a data breach, including but not limited to tracking, reporting, assessing, and determining eligible data breach status, management activities, communications and notifications will be managed in line with the *Public Records Act 2023.*

Record keeping practices will align with the CQHHS QPP Privacy Policy to ensure the privacy of affected individuals is maintained.

Related Legislation and Standards

The CQHHS has considered, referenced, and utilised various legislation and standards in the development of our policies and procedures.

- Information Privacy Act 2009 and the Queensland Privacy Principles
- Hospital and Health Boards Act 2011
- Public Records Act 2023

- Mental Health Act 2016
- Public Interest Disclosures Act 2010
- Crime and Corruption Act 2001
- Child Protection Act 1999
- Human Rights Act 2019
- Public Health Act 2005
- Security of Critical Infrastructure Act 2018 (Cth)
- Privacy Act 1988 (Cth)
- National Safety & Quality Health Service Standards
- NSQHS Standard 1 - Clinical Governance
- NSQHS Standard 2 - Partnering with Consumers
- Aged Care Quality & Safety Commission Standard 8 – Organisational Governance
- Code of Conduct for the Queensland Public Service
- Australian Charter of Healthcare Rights