Data Breach Procedure

Gold Coast Hospital and Health Service

Data Breach Procedure

Published by the State of Queensland (Queensland Health), June 2025

For more information contact:
Right to Information and Privacy, Gold Coast Hospital and Health Service, 1 Hospital Boulevard, Southport QLD 4215, email GCHHSPrivacy@health.qld.gov.au.

Purpose

This procedure describes the process for GCHHS's management of a confirmed or suspected data breach.

What is a data breach?

A ***data breach*** occurs if there is:

a. *unauthorised access to or unauthorised disclosure of the information.*
b. *the loss of the information in circumstances where authorised access to, or unauthorised disclosure of the information is likely to occur.*

As defined in Schedule 5 of the *Information Privacy Act 2009* (Qld).

A data breach is also an ***eligible data breach*** if both of the following apply:

a. there is unauthorised access to, or unauthorised disclosure of, personal information held by the agency, or there is a loss of personal information held by the agency in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and
b. the unauthorised access or disclosure of the information is likely to result in serious harm to an individual.

As defined by section 47 of the *Information Privacy Act 2009* (Qld).
If a data breach is assessed as an ***eligible data breach*** the mandatory notification of data breach (**MNDB**) scheme obligations will apply. Refer to paragraph 9Z for more information on the MNDB obligations.

Identifying a data breach

How to identify a data breach:

A data breach can occur in a range of different ways, including but not limited to:

- loss or theft of physical devices or paper records;
- overprovisioning of access to software or data recording systems;
- unauthorised access;
- inadvertent disclosure or deliberate disclosure; or
- hacking or phishing.

What happens if you identify a data breach?

GCHHS Employees
If a GCHHS employee discovers, or is alerted by another agency, system, or person, to a perceived or actual data breach, the employee is required to contact the Privacy and Confidentiality Contact Officer (**PCCO**) at GCHHSPrivacy@health.qld.gov.au providing as much information about the breach as possible.

Contracted Service Providers
Any agency that has a contract or agreement with GCHHS and collects, uses, accesses, discloses, or stores data on behalf of GCHHS is responsible for reporting breaches to GCHHS in accordance with the contracted agreement. All breaches must be reported to the GCHHS representative defined in the contract as soon as the breach has been identified. That GCHHS representative is then obliged to immediately report internally as detailed above.

Public
Should any member of the public, whether a patient or otherwise, raise concerns about an actual or perceived data breach of any type (whether perceived or actual) the individual is advised to contact GCHHSPrivacy@health.qld.gov.au with their concerns.

Investigating a data breach

The recipient of the breach notification will liaise with the person/s who identified the breach to collect information, including:

- time, location and context of the breach;
- the cause of the breach;
- the type/s of personal information that has been accessed, disclosed, and/or lost;
- whether there are audit logs or other records held by the relevant IT systems;
- the extent of the breach; and
- whether there are relevant stakeholders (including other government agencies, third parties, or internal business areas).

If the recipient suspects an eligible data breach has occurred, the recipient will escalate to the Data Breach Group and a meeting will be scheduled immediately. Any of the following positions can stand up the Data Breach Group upon receipt of a submitted form or other notifiable process:

Standing members

- Senior Director, Health Information
- Senior Director, Digital Security and Architecture
- Director, Corporate Governance
- Senior Director, Strategic Communication and Engagement
- Manager, Right to Information and Privacy (PCCO)
- General Counsel or Legal Services (as appropriate)
- Senior Director, Technology Operations (as appropriate)
- Senior Director, Digital Experience (as appropriate)
- Executive Director, Digital and Information (as appropriate)

Containing a data breach

Any immediate steps available to contain the breach must be identified and implemented by the line manager of the impacted area. A nominated position from the Data Breach Group will assist the relevant line manager to ensure appropriate containment is undertaken.

The Data Breach Group may identify and direct implementation of further mitigation actions. It is expected that agencies acting on behalf of GCHHS will take steps to correct, remediate and/or resolve the issue where applicable and appropriate, and fully cooperate with any GCHHS investigation.

Assessing a data breach

The Data Breach Group will conduct an assessment on whether the data breach meets the threshold for an eligible data breach. It must be noted that the approach to identifying, assessing, and responding to data breaches will be dependent on the nature of the breach.

Once this information about the context of the data breach has been obtained, the PCCO will assess the potential impact on affected individuals, including:

- actual or potential harms to individuals whom the personal information relates to;
- the seriousness of that harm; and
- the likelihood that the harm will occur.

When determining the likelihood of serious harm, the PCCO will assess the matters established in section 47(2) of the IP Act:

- the kind of personal information accessed, disclosed or lost;
- the sensitivity of the personal information;
- whether the personal information is protected by one or more security measures;
- if the personal information is protected by one or more security measures, the likelihood that any of those security measures could be overcome;
- the person or the kinds of persons, who have obtained or could obtain the personal information;
- the nature of the harm likely to result from the data breach; and
- any other relevant matters.

If the above assessment supports that there is a likelihood of serious harm resulting from the data breach, the MNDB scheme obligations may apply.

Assessing Data Breaches involving other agencies

If at any time, GCHHS is made aware that an eligible or suspected eligible data breach affects another agency, GCHHS will provide written notice to the other agency informing them of the data breach and a description of the potential personal information involved in the breach.

Mitigating a data breach

The Data Breach Group will identify and take all reasonable remediation steps to mitigate the harm caused by the data breach. Remediations steps will be documented by the Data Breach Group and acted upon as soon as possible.

Additionally, the line manager of the impacted area must take all reasonable steps to eliminate the circumstances enabling the beach to occur.

Remediation steps may include:

- making efforts to recover the personal information;
- securing, restricting access, or shutting down to breached systems;
- enhanced physical and technical security controls;
- suspending the activity that led to the data breach;
- information sharing agreements;
- creating or updating policies and procedures;
- arranging support for individuals impacted by the breach;
- escalation to the GCHHS Health Incident Controller; and/or
- revoking or changing access codes or passwords.

Notifications

If the Data Breach Group is satisfied that their analysis supports a reasonable belief that there has been an eligible data breach, the obligations to notify the Information Commissioner and Particular Individuals apply.

Notification to Office of the Information Commissioner (OIC)

If an eligible data breach occurs, GCHHS will notify the Information Commissioner as soon as practicable. As required by section 51 of the IP Act, the PCCO will provide the Information Commissioner with a written notice, including:

- contact details of nominated contact person for GCHHS;
- if more than one agency is affected by the data breach;
- whether GCHHS is reporting on behalf of another agency;
- the date of the data breach;
- a description of the data breach, including the type of eligible data breach under section 47;
- a description of the kind of personal information involved in the data breach;
- information regarding how the data breach occurred;
- if the data breach involved unauthorised access to or disclosure of personal information, the period during which the access or disclosure was available or made;
- the steps GCHHS has taken or will take to contain the data breach and mitigate any potential harm caused by the data breach;
- GCHHS's recommendations about the steps individuals should take in response to the data breach;
- the total number or an estimation of the total number of individuals whose personal information was accessed, disclosed or lost;
- whether the notified individuals have been advised how to make a privacy complaint to the agency under section 166A; and
- the total number of individuals notified of the data breach.

Notifications to Particular Individuals

As soon as GCHHS has reasonable belief that a data breach is an eligible data breach, GCHHS will notify particular individuals as required under section 53 of the IP Act. In accordance with section 53(2), the PCCO will provide the affected individuals with a written notice, including:

- a summary of the incident;
- a description of their affected personal information;
- containment and mitigation steps taken by GCHHS to prevent further harm;
- risk of harm involving health, financial or identity information;
- contact details of the agency or person nominated by the agency; and
- process for making a privacy complaint under section 166A.

Additional Notification or Reporting Obligations

Additional notification and reporting obligations may apply, as per *Appendix 1.*

If required, the Data Custodian or delegate will be contacted to notify the governing body. If the breach is escalated to a governing agency, further preventative and remedial actions may be recommended post assessment.

In the event that a data breach is the result of a Cyber Security Incident, the requirements for reporting to the Australian Cyber Security Centre outlined within the HHS's internal procedures will also apply.

When appropriate, or as governed, GCHHS will also consider notification to:

- Queensland Police Service;
- Crime and Corruption Commission Queensland (through the GCHHS Ethical Standards Unit);
- Queensland Government Insurance Fund (QGIF);
- Queensland Government Chief Information Officer;
- the Office of the Australian Information Commissioner;
- Australian Federal Police;
- the Australian Taxation Office;
- the Australian Digital Health Agency;
- any third-party organisations or agencies whose data may be affected;
- financial services providers;
- professional associations, regulatory bodies, or insurers; and/or
- foreign regulatory agencies.

Review and evaluate

The Data Breach Group will undertake audits to ensure follow-up actions and improvements have been implemented by relevant line managers. The Data Breach Group will undertake post-response assessments of the organisations' responsiveness to the breach and effectiveness of this procedure. Lessons learnt from the post-response assessment will be used to inform quality improvement activities.

Data Breach Register

In accordance with section 72 of the IP Act, GCHHS holds and maintains an internal register of eligible data breaches. The register details the below information, as required by section 72(2):

- date of breach;
- description of data breach;
- date notification provided to OIC;
- date additional information provided to OIC;
- individuals notified, including date and method;
- details of any exemptions relied on or N/A;
- steps taken to contain and mitigate; and
- actions taken to prevent similar breaches.

Roles and responsibilities

Roles	Responsibilities
Third party agency	• Report breach to GCHHS in accordance with contracted conditions.
Staff Member	• Refer to the procedure and take immediate action. • Email GCHHSPrivacy@health.qld.gov.au to notify the PCCO of the breach and inform them regarding the circumstances relating to the breach. • Where possible, notify Line Manager/Delegate of known or suspected breach.
Line Manager	• Register the breach in RiskMan. • Take steps to contain the breach (if appropriate). • Document initial remediation activities (if appropriate). • Implement post-breach review findings.
Privacy and Confidentiality Contact Officer (PCCO)	• Assess if the breach is an eligible data breach. • Escalate eligible or suspected eligible breaches to the Data Breach Group. • Identify if external notification is required; persons affected and/or Office of the Information Commissioner. • Facilitate notification process, if required. • Standing member in the Data Breach Group. • Maintain Internal Data Breach Register
Strategic Communication and Engagement	• Escalate eligible or suspected eligible breaches to the Data Breach Group. • Determine if internal and external communications are appropriate. • Standing member in the Data Breach Group.
Data Breach Group	• Maintain a data breach register of all reported actual and potential breaches. • Provide support and guidance to staff, line managers and Custodians, as needed. • Determine whether there has been a potential breach. • Determine scope and possible impact of the potential breach. • Escalate to the Health Incident Controller who has overall responsibility for incidents within the HHS if appropriate. • Provide situation reports and advice to the Health Emergency Operations Centre (HEOC) meetings. • Seek assistance from internal/external stakeholders e.g., for reputational and contractual advice and remediation. • Identify actions to remediate the breach. • Identify if external notification is required to relevant governing bodies. • Undertake post-breach review. • Maintain a record of breaches, investigations, actions, and resolution.
Health Information	• Assess the if the breach is eligible. • Escalate eligible or suspected eligible breaches to the Data Breach Group. • Standing member in the Data Breach Group.

HEOC	• Incident Management Team – Senior leaders within the HHS responsible for the management of incidents
Health Incident Controller	• Delegated responsibility of the Chief Executive to manage Level 3 incidents across the HHS
Corporate Governance	• Assess the if the breach is eligible. • Escalate eligible or suspected eligible breaches to the Data Breach Group. • Standing member in the Data Breach Group
Information Security and Cyber Readiness	• Assess the if the breach is eligible. • Escalate eligible or suspected eligible breaches to the Data Breach Group. • Standing member in the Data Breach Group.
Data Custodian	• Fulfill responsibilities of Data Custodian • Notify external agencies of the breach, as required by procedure and legislative requirements.
Executive Director, Corporate Affairs	• Deliver updates to the Executive Leadership Team. • Undertake mandatory reporting to the Australian Cyber Security Centre, if required.
Executive Director, Digital Transformation and Research	• Deliver updates to the Executive Leadership Team.

Definition of Terms

Term	Definition	Source
Personal Information	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.	Section 12 of the *Information Privacy Act 2009* (Qld)
An agency *held or holds* personal information	Personal information is held by a relevant entity, or the entity holds personal information, if the personal information is contained in a document in the possession, or under the control, of the relevant entity.	Section 13 of the *Information Privacy Act 2009* (Qld)
Data	Includes information in any form.	*Security of Critical Infrastructure Act 2018* (Cth)
Data Custodian	A position designated with overall accountability and responsibility for decision making in relation to the data set, data collection and/or application allocated and the ongoing capture, compliance, development, management, care, and maintenance of data to support business needs.	Data and application custodianship roles and responsibilities
Data breach	A 'data breach' means either of the following in relation to information held by an agency:	Schedule 5 of the *Information Privacy Act 2009* (Qld)

	(a) unauthorised access to, or unauthorised disclosure of, the information. (b) the loss of the information in circumstances where unauthorised access to, or unauthorised disclosure of the information is likely to occur	
Eligible data breach	A data breach is an eligible data breach if both of the following apply: (a) there is unauthorised access to, or unauthorised disclosure of, personal information held by the agency, or there is a loss of personal information held by the agency in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur, and (b) the unauthorised access or disclosure of the information is likely to result in serious harm to an individual.	Section 47 of the *Information Privacy Act 2009* (Qld)
Serious harm	Serious harm occurs if there is serious physical, psychological, emotional, or financial harm to the individual because of the access or disclosure; or serious harm to the individual's reputation because of the access or disclosure.	Schedule 5 of the *Information Privacy Act 2009* (Qld)

Cyber security incident	An unwanted or unexpected event caused by a possible breach of security procedure, failure of safeguards or an unknown situation that has either compromised business operations or has a significant probability of compromising business operations.	Australian Signals Directorate – Guidelines for Cyber Security Incidents