# Policy

Document ID: 001774 Version: 1.0

# Data Breach

Date Approved: 03/06/2025 Review Date: 03/06/2027

## Policy Statement

Sunshine Coast Health takes the protection of privacy seriously. The purpose of this policy is to provide an overview of Sunshine Coast Health's procedures and processes in relation to containing, assessing, managing, notifying, and reporting on eligible data breaches in accordance with the Mandatory Notification of Data Breach Scheme (the MNDB Scheme) as established by the *Information Privacy Act 2009 (Qld)* (the IP Act).

This policy complies with section 73 of the IP Act.

## Scope and target audience

This policy applies to:

- All permanent full time, part time, temporary and casual employees in accordance with Queensland Health Employment Framework (QH-POL-205) authorised to access Sunshine Coast Health information systems and assets.
- Any volunteers, contracted service providers, consultants (including Visiting Medical Officers), students and persons or organisations authorised to administer, develop, manage and support Sunshine Coast Health information systems and assets.

### Data breach and eligible data breach

A data breach occurs when personal, confidential, sensitive, or protected information, including health information, held by Sunshine Coast Health is lost or subject to unauthorised access or disclosure.

A data breach may be malicious, the result of human error or a failure of information systems or security systems.

Types of data breaches include but are not limited to:

- Loss or theft of Sunshine Coast Health information or device containing sensitive information, such as a USB stick, laptop, file or mobile phone.
- Compromise or unauthorised access to an information database, for example, through sharing user login details with a third party, hacking or malware infection.
- An employee or contractor mistakenly providing personal information to an unauthorised person or entity, such as sending an email containing personal information to the wrong recipient.

Under section 47 of the IP Act, for a data breach to be an 'eligible data breach' triggering notification and obligations under the MNDB scheme, both of the following must apply:

1. 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
2. the unauthorised access or disclosure of the information is likely to result in serious harm to an individual.

Serious harm occurs when the breach has, or may have, a real and substantial detrimental effect on an individual. This harm can be physical, economic, financial, social, emotional, psychological, or reputational.

The assessment of the likelihood of serious harm arising from a data breach is an objective test.

## Data Breach Response Plan

Sunshine Coast Health has implemented a comprehensive data breach response plan, to ensure swift and effective action in the event of a data breach. Employees are expected to familiarise themselves with this plan and the associated requirements. The data breach response plan is tested annually.

## Privacy Policy

The principles outlined in the health service Privacy Policy apply to this policy.

## Response and management strategy

Sunshine Coast Health employees are required to complete mandatory e-learning modules:

1. Code of Conduct (Annually)
2. Cyber Security Essentials (Annually)
3. ieMR Confidentiality (for system users).

These mandatory training modules ensure employees have the necessary understanding of what a data breach is, what is required of them and to be able to respond accordingly. All employees should consult the Sunshine Coast Health data breach response plan for further detailed guidance on how to respond to a data breach located on our employee intranet.

All Sunshine Coast Health employees, contracted service providers, consultants and volunteers are to immediately notify the Health Service of any data breach or suspicion of involving the accidental or malicious loss, disclosure or corruption of Sunshine Coast Health information.

Cyber Security Group (CSG) in eHealth Queensland proactively identifies data breaches that may impact Sunshine Coast Health by actively monitoring public domains for cyber threats. In an emerging and evolving threat environment the health services are notified of cyber alerts for potential vulnerabilities in our environment that Sunshine Coast Health Strategy and Architecture team investigate and monitor.

Internally if a data breach occurs, employees are immediately required to take all steps to prevent any further impact of the data breach and follow the data breach response plan. Priority needs to be taken to reduce any further loss, or compromise of personal, sensitive or health information and minimise any potential harm to affected individuals.

Sunshine Coast Health business units are to refer to the data breach response plan to make an initial assessment as to whether the breach meets the eligibility criteria under the MNDB scheme. Where further guidance is required, refer to the Principal Privacy Officer.

If members of the community of become aware of data breach impacting Sunshine Coast Health data or systems, they can email SCHHS_PRIVACY@health.qld.gov.au

## Data Breach Response Team

In the event of an eligible data breach, Sunshine Coast Health may convene the data breach response team.

The response team leaders (Executive Director of Legal and Governance and Chief Digital Officer) will decide whether to convene the response team.

The response team consists of:

- Executive Director Legal and Governance
- Chief Digital Officer
- Principal Privacy Officer
- Senior Director, Communications and Engagement
- Manager, ICT Strategy and Architecture (where a Cyber Incident has occurred)
- Nursing Director, Safety and Quality Unit
- Director Digital Health and Clinical Information Services
- Director Workforce Advisory, Workforce
- Affected business unit/s.

The response team will carry out a comprehensive evaluation of any suspected eligible data breach, considering the following factors:

- The root cause of the breach and containment action.
- The potential risk of serious harm to affected individuals, and recommended measures to mitigate this risk.
- The requirements to notify affected individuals and if so, the communications approach.
- Notification to the Queensland Information Commissioner as required by sections 51 and 52 of the IP Act.
- Where relevant, depending on the nature and severity of the incident, notification of other external authorities and agencies, for example:
  - Queensland Police
  - Australian Digital Health Agency
  - Queensland Government Cyber Security Unit
  - Crime and Corruption Commission Queensland
  - Office of the Australian Information Commissioner

Further comprehensive details on management following the four key steps of ***contain, assess, notify, and review*** and post incident reporting can be located in the data breach response plan.

### Data Breach communications strategy

To meet the requirements of the MNDB scheme, Sunshine Coast Health will developed a communications strategy in the event of an eligible data breach.

The Senior Director, Communications and Engagement is responsible for the oversight of the communication plan specific to the requirements of an eligible data breach as part of the data breach response plan.

### Post-breach review and evaluation

The Principal Privacy Officer with the support of the affected business unit/s, must conduct a post-breach review and evaluation of eligible data breaches to:

- Identify if there are weakness in processes, systems, or activities that may have contributed to the breach.
- Assess the effectiveness of the health services data breach response activities.
- If required, develop a proposed action plan of preventative measures and mitigation strategies to be put in place for each identified weakness for the approval of the Health Service Chief Executive.

## Data Breach Register

Sunshine Coast Health will maintain an internal register of all data breaches as required by section 72 of the IP Act. This Data breach register meets the specific information requirements set forth in section 72(2). This register is managed by the Principal Privacy Officer.

## Definition of key terms

| Term | Description |
|---|---|
| Data Breach | A 'data breach' means either of the following in relation to information held by an agency:<br>(a) unauthorised access to, or unauthorised disclosure of, the information.<br>(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 | 1. 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<br>2. the unauthorised access or disclosure of the information is likely to result in serious harm to an individual. |
| Data Breach Response Team | Responsible for carrying out the actions that can reduce the potential impact of an eligible data breach. |
| *Information Privacy Act 2009 (Qld)* (IP Act) | The Information Privacy Act 2009 Qld) (IP Act) recognises the importance of protecting personal information of individuals. It contains a set of 'privacy principles' that govern how Queensland Government agencies collect, store, use and disclose personal information. |
| Mandatory Notification Data Breach Scheme (MNDB) | Under Chapter 3A of the IP Act, Queensland Government agencies are required to deal with personal information in compliance with the mandatory notification of data breach scheme. |
| 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—<br>(a) whether the information or opinion is true or not; and<br>(b) whether the information or opinion is recorded in a material form or not. |

## References and further reading

**Primary legislation, policy, standards or other authority**

*Information Privacy Act Qld 2009 (Qld)*

*Security of Critical Infrastructure Act 2018 (SOCI)*

QH-POL-205 Queensland Health Employment Framework

Information security classification framework (QGISCF) | For government | Queensland Government

Sunshine Coast Health Privacy Policy

**National Safety and Quality Health Service (NSQHS) Standards 2nd ed**

- Clinical Governance
- Partnering with Consumers

**Forms and other related or supporting documents**

Reporting a privacy breach | Office of the Information Commissioner Queensland

Report a Cyber security incident – Queensland Government

Reporting Corruption | CCC - Crime and Corruption Commission Queensland

Policelink - Reporting | QPS

Report a data breach | OAIC

Home - Queensland Government Insurance Fund (QGIF)

Queensland Health Employment Framework

## Consultation

Key stakeholders who contributed to and/ or reviewed this version include:

Executive Director Legal and Governance

Chief Digital Officer

Senior Director, Communications and Engagement

Director, Digital Health, and Clinical Information Services

Director, Workforce Advisory

Director, Internal Audit

Nursing Director, Safety and Quality Unit

Manager, ICT Strategy and Architecture

Manager, Risk

Manager, Clinical Informatics Operations

Lead Health Information Manager

Principal Privacy Officer

Principal Advisor, Ethics, and Integrity

Senior Coordinator, Clinical Information Access

## Compliance

☐ Existing Sunshine Coast Health Audit: N/A

☐ Department or Sunshine Coast Health Quality program: N/A

☒ Reporting mechanism: Privacy Report, Executive Audit and Risk Committee

☐ Key indicators and/ or outcomes: N/A

## Document approval

| Version | Prepared by | Endorsed by | Authorised by | Review due |
|---|---|---|---|---|
| 1.0 | Principal Privacy Officer | Governance Improvement Committee | Executive Director, Legal and Governance | 03/06/2027 |
| **Approved by:** Sunshine Coast Hospital and Health Board 03/06/2025 | | | | |
| **Supersedes:** N/A | | | | |
| **Keywords:** data breach, privacy, confidentiality, MNDB, eligible data breach, data breach policy, data breach response plan, data breach response team, privacy breach, information privacy, data | | | | |