West Moreton Health

Data Breach Policy

Caring Better Together

Queensland Government

Published by the State of Queensland (Queensland Health), June 2026.

For more information, contact:
Privacy, Legal Services, West Moreton Hospital and Health Service
PO Box 73, Ipswich Hospital, Ipswich QLD 4305

Policy statement

West Moreton Hospital and Health Service (**West Moreton Health**) is committed to protecting personal information and responding effectively to data breaches. West Moreton Health will take reasonable steps to contain, assess, and manage all data breaches and comply with its notification obligations under the *Information Privacy Act (Qld)* (**IP Act**) and its Queensland Privacy Principles (**QPPs**).

Purpose

The IP Act regulates how Queensland government agencies, such as West Moreton Health must comply with the requirements of the Mandatory Notification Data Breach (**MNDB**) Scheme.

This policy outlines West Moreton Health's approach to identifying, managing, and responding to data breaches in accordance with the IP Act, including the MNDB Scheme.

Data breach

A data breach occurs when information held[1] by West Moreton Health is accessed or disclosed without authorisation or is lost in circumstances where unauthorised access or disclosure is likely to occur[2].

A data breach can involve any type of information.

Data breaches may occur due to:

- malicious actions (by external or internal parties);
- human error; or
- failures in systems, processes, or information security controls.

Examples of data breaches include:

- phishing emails that trick a user into providing information or access;
- sending information to the wrong recipient;
- leaving information in a public place;
- lost or stolen devices, storage media, or paper records; or
- staff accessing information without a valid work-related purpose.

Eligible data breach

An eligible data breach is a data breach where unauthorised access, disclosure, or loss of personal information occurs, and unauthorised access or disclosure is likely. It must also be likely that the incident will result in serious harm to an individual.

Personal information

Personal information is any information or opinion about an identified individual or an individual who is reasonably identifiable. It applies whether the information is true or not, and whether it is recorded in a material form or not.[3]

[1] Defined in section 13 the IP Act
[2] Defined in schedule 5 of the IP Act
[3] Defined in section 12 of the IP Act

Unauthorised access, disclosure and loss

A data breach can happen in different ways, including when information is accessed, shared, or lost without permission.

Unauthorised access

This happens when personal information is viewed or accessed by someone who is not allowed to see it.

Examples include:

- a staff member looking at records without a work-related reason
- using system access for purposes outside a project or role
- external parties accessing information during a cyber incident

Unauthorised disclosure

This happens when personal information is shared without proper approval, either by mistake or on purpose.

Examples include:

- publishing information online accidentally
- emailing personal information to the wrong person
- sharing information that still includes identifying details
- systems that allow people to see information they should not access

Unauthorised access and disclosure can happen at the same time. For example, if information is accidentally made public online, it may be both shared without permission and accessed by others.

Loss of personal information

This happens when information is lost or no longer under the control of West Moreton Health.

Examples include:

- losing devices or paper records
- disposing of equipment that still contains personal information
- theft of devices from workplaces or homes

Loss is only considered a data breach if it is likely that the information could be accessed or shared without permission.

Serious harm and risk assessment

West Moreton Health applies a risk-based approach to determine whether a data breach is likely to result in serious harm[4].

Serious harm

Serious harm must be more than minor inconvenience or embarrassment and may include:

- financial loss or identity theft
- emotional distress
- reputational damage
- risks to personal safety

A data breach involving personal information will be considered an eligible data breach where serious harm to one or more individuals is likely.

[4] Defined in schedule 5 of the IP Act

Serious harm is considered likely where the risk is more probable than not based on the circumstances. It is not necessary to identify every affected individual for this threshold to be met. Where there is uncertainty, West Moreton Health takes a precautionary approach and may treat the breach as likely to result in serious harm.

Likely to result

In assessing whether a data breach is likely to result in serious harm, West Moreton Health will consider factors such as:

- the type and sensitivity of the personal information involved
- whether the information was protected by security measures (for example, encryption) and how effective those measures are
- the likelihood that any security protections could be overcome
- who has accessed, or could access, the information
- the nature and extent of the potential harm to individuals
- any other relevant circumstances

Data breach response framework

West Moreton Health will maintain appropriate systems, policies, and procedures to support effective data breach response, including staff training, defined roles and responsibilities, and access to specialist expertise where required.

West Moreton Health responds to all data breaches using a structured and consistent 5-stage approach:

1. **Identify** the data breach
2. **Contain and mitigate** risks and impacts
3. **Assess** the nature and severity of the breach
4. **Notify** where required
5. **Review** to support improvement

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?

All suspected or confirmed data breaches should be reported as soon as practicable so they can be assessed and managed appropriately.

West Moreton Health Employees

If a West Moreton Health employee discovers, or is alerted by another agency, system, or person, to a suspected or actual data breach, the employee is required to immediately contact the WM Privacy and Confidentiality Contact Officer (**PCCO**) and their line manager providing as much information about the breach as possible.

Contracted Service Providers

Any contractor or third party service provider handling information on behalf of West Moreton Health must report any data breaches to West Moreton Health as soon as they are identified, in accordance with contractual requirements. The nominated West Moreton Health representative must then ensure the breach is promptly reported internally.

Public

Should any member of the public, whether a patient or otherwise, have any concerns about privacy or how their personal information is handled, they are encouraged to contact the Consumer Liaison Office (**CLO**) at WMH_CLO@health.qld.gov.au with their concerns.
CLO will collaborate with the WM PCCO to review the matter.

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 the personal information
- securing, restricting access to, or shutting down breached systems in consultation with West Moreton Health Information Security and Cybersecurity
- suspending the activity that led to the data breach
- revoking or changing access codes or passwords.

The business area affected by the data breach will work with WM Privacy and any other relevant business areas to take appropriate steps to contain the breach and reduce any potential harm. There is an immediate and ongoing responsibility to contain the breach and minimise risks while the incident is assessed and managed.

Specialist support may also be involved where needed, such as information technology or cyber security teams, to assist in containing and managing the data breach.

Deciding what actions to take

In determining the most appropriate response, the following questions may be considered:

- What caused the data breach, and can temporary controls be put in place to prevent further impact?
- Is it necessary to work with third parties or service providers to investigate and resolve the issue?
- Can the personal information be recovered?
- Can the person who received the information in error be contacted?
- Can access to the affected system be restricted or the system shut down?

What you should do

If you think your information has been involved in a data breach:

- contact West Moreton Health
- follow any advice provided in notifications
- consider steps such as monitoring accounts or updating passwords

Assessment

West Moreton Health will assess all suspected data breaches to determine whether they meet the threshold of an eligible data breach under the MNDB scheme. This involves gathering relevant information and evaluating the potential risks to individuals.

As part of this process, West Moreton Health will:

- collect key details about the breach, including the type of information involved and the number of individuals affected
- assess the likelihood of serious harm to impacted individuals
- consider whether the available information supports a reasonable suspicion or belief that the breach is eligible

In making this assessment, West Moreton Health will consider factors such as:

- the sensitivity and type of personal information involved
- who may have accessed or received the information
- how the breach occurred
- whether security measures were in place and their effectiveness
- the potential impact on affected individuals

West Moreton Health may also seek advice from relevant internal or external experts, such as information security, legal services, or law enforcement, to support decision-making and ensure an appropriate response.

If an eligible data breach is suspected, West Moreton Health may stand up an established dedicated response team, including senior staff and subject matter experts, to manage significant data breaches.

The personnel involved in a particular data breach will vary depending on the specific nature and scope of the breach.

Notification

Where West Moreton Health reasonably believes an eligible data breach has occurred, it will notify, as soon as practicable:

- the Queensland Information Commissioner
- affected individuals, unless an exemption applies

Notification methods will be determined on a case-by-case basis and may include direct communication (such as email, letter, or telephone) or publication on the West Moreton Health website where appropriate.

West Moreton Health may also notify other agencies or organisations where relevant, including where:

- other agencies are affected
- Tax File Numbers are involved
- regulatory, legal or contractual obligations apply
- there is a need to involve entities such as law enforcement or oversight bodies

Information provided in notifications

Notifications will include appropriate information to support transparency and enable individuals to take protective action. This may include:

- a description of the breach, including when and how it occurred
- the type of personal information involved
- the period of any unauthorised access or disclosure
- steps taken by West Moreton Health to contain the breach and reduce harm
- recommended actions individuals can take in response
- contact details and information on how to make a privacy complaint

Where required, additional information may be provided to regulators, including details about the number of individuals affected and the steps taken in response.

Notifying particular individuals

If another agency is affected, West Moreton Health will provide written notice as appropriate, including:

- details of the breach
- the types of information involved
- actions taken to manage the incident
- relevant contact information

Exemptions

The MNDB Scheme includes limited exemptions from notification requirements. Where an exemption applies, West Moreton Health will manage the breach in accordance with legislative obligations.

Review and evaluation

After a data breach has been managed, West Moreton Health will conduct a review to identify lessons learned and reduce the risk of future incidents. The scope of the review will depend on the seriousness of the breach and may involve relevant staff and members of the Data Breach Group.

The review focuses on understanding the cause of the breach, assessing how effectively it was managed, and identifying any improvements needed to policies, processes, or systems. Actions may include strengthening safeguards, enhancing staff training, and improving data handling practices.

West Moreton Health also undertakes monitoring and follow-up activities to ensure improvements are implemented and effective. Findings from the review are documented and used to support continuous improvement and strengthen the organisation's approach to data protection.

Recordkeeping

West Moreton Health will:

- maintain records of data breaches, including assessments of whether a breach is an eligible data breach, in accordance with the *Public Records Act 2023*
- keep an internal register of eligible data breaches in line with section 72 of the *Information Privacy Act 2009*
- securely store all data breach records and related documentation

West Moreton Health uses secure systems to protect personal information and takes all reasonable steps to prevent misuse, interference, loss, and unauthorised access, modification, or disclosure.

Preventative measures

West Moreton Health has a range of measures in place to reduce the risk of data breaches and strengthen the protection of personal information. These include:

- a comprehensive data governance framework supported by policies and procedures, including privacy, records management, and information security policies
- cyber security and privacy training to support staff in protecting personal information and reducing the risk of security incidents
- an Information Security Management System (ISMS) aligned with recognised standards (such as ISO 27001)
- ongoing privacy awareness initiatives to support appropriate collection, use and disclosure of personal information
- contractual arrangements with third-party service providers that include clear privacy obligations, data breach reporting requirements, and secure data handling and disposal provisions

Feedback

West Moreton Health welcomes feedback on this Data Breach Policy and is committed to continuous improvement.

Definition of terms used in this policy

Term	Definition
Personal Information *Defined in section 12 the 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.
An agency held or holds personal information *Defined in schedule 5 of the IP Act*	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.
Data breach *Defined in section 13 the IP Act*	A 'data breach' means either of the following in relation to information held by an agency: (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 *Defined in section 47 the IP Act*	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.
Serious harm *Defined in schedule 5 of the IP Act*	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.