POLICY

Document ID: WBHHS-POL-2574

Data Breach Policy

1. Policy statement

Wide Bay Hospital and Health Service (WBHHS) is committed to the protection of personal information through the preparation, identification, containment and mitigation, assessment and notification of data breaches including suspected eligible data breaches.

The policy aims to enforce HHS wide individual accountability for safeguarding personal information, promptly responding to data breaches and taking proactive steps to mitigate harm.

It is supported by the WBHHS Data Breach Response Plan that provides more detailed instruction on responding to a data breach and the WBHHS QPP Privacy Policy

2. Scope

This Policy relates to all WBHHS employees (permanent, temporary and casual) and all organisations and individuals acting as its agents, including Visiting Medical Officers and other partners, contractors, consultants, students and volunteers in the Service.

3. What is a data breach

Data breach

A data breach occurs when there is unauthorised access or disclosure of personal information; or a loss of personal or non-personal information held by the WBHHS where disclosure is likely to occur.

Data breaches can occur because of a technical problem, human error, inadequate policies and training, a misunderstanding of the law, or a deliberate act. Some of the more common privacy breaches happen when personal information is lost or mistakenly disclosed (for example, a USB flash drive or laptop is lost or stolen, or patient related correspondence is sent to unintended recipients).

A data breach may or may not result in notification to the Office of the Information Commissioner (OIC).

Refer to Appendix A for examples.

Eligible data breach

An “Eligible Data Breach” will have occurred under section 47 of the IP Act where:

(a) there has been unauthorised access to, or unauthorised disclosure of personal information held by WBHHS, and the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates; or

(b) there has been loss of personal information held by WBHHS that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, and the loss is likely to result in serious harm to any of the individuals to whom the information relates.

Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion:

- Whether the information or opinion is true or not; and

- Whether the information or opinion is recorded in a material form or not.

Personal information held by WBHHS means it is contained in a document in the possession or under the control of WBHHS. This may include documents stored in IT systems or paper files and can include documents held by contracted service providers.

Serious harm *is* defined as including:

- Serious physical, psychological, emotional, or financial harm to the individual because of the access or disclosure
- Serious harm to the individual's reputation because of the access or disclosure

It is a legislative requirement for the WBHHS to report an eligible data breach to the OIC under the Mandatory Notification of Data Breach (MNDB) scheme.

Reasonable Suspicion and Reasonable Belief of a Data Breach

Reasonable suspicion means insufficient information exists to confirm a data breach as an eligible data breach and further investigation maybe required to determine reasonable belief.

Reasonable belief means sufficient information exists to confirm a data breach is an eligible data breach.

3.1 Data Breach Management

Data breach management is a requirement of the Mandatory Notification of Data Breach **(**MNDB) scheme under Chapter 3A of the *Information Privacy Act 2009* (QLD) (IP **Act**). It involves identifying, assessing, containing and mitigating data breaches to minimise harm to individuals and WBHHS.

The MNDB scheme places an obligation on WBHHS to determine if the breach is an eligible data breach and as soon as practicable notify the OIC and affected individuals.

Contractors bound to the QPPs assume the privacy obligations of WBHHS and in the event of a breach, must notify WBHHS of the data breach, investigations taken and outcomes. Appropriate notifications to the OIC or other agencies as required under legislation remains the responsibility of WBHHS.

Preparing for a data breach

In addition to this Data Breach policy, to support the management of data breaches WBHHS maintains and adheres to several documents including the:

- WBHHS Privacy Policy
- WBHHS Data Breach Response Plan
- WBHHS Data Breach Register
- WBHHS Information Security Procedure
- Queensland Health Information Security Policy
- Queensland Health Use of ICT Services and Devices Policy
- Queensland Government Information Security Policy (IS18)

Key WBHHS personnel assist in the investigation and reporting of data breaches including the:

- Privacy and Confidentiality Contact Officer (PCCO) as the primary point of contact for reporting data breaches.
- Data Breach Response Team (DBRT), consisting of subject matters experts from Legal Services, Information Management, ICT, Risk and Compliance, Human Resource Management and Clinical Governance. The DBRT may assist with investigation, recommending remediation strategies and/or actioning remediation strategies.

Mandatory and non-mandatory privacy and cyber security training is available via WBHHS and Queensland Health learning management systems. Compliance with mandatory training is to be monitored and managed by individual employees, line managers, and data and application custodians.

WBHHS uses several systems and processes to monitor and maintain information security. This includes

- Information Security Management System (ISMS)
- User access management and sentinel reporting across digital information systems
- Defined roles and responsibilities for information security
- Use of data sharing agreements
- Use of privacy impact assessments
- Business continuity plans including systems backup and restore
- Penetration testing (simulated cyber-attack) on computer systems
- Cyber incident response plan.

Responding to a data breach

Responding to a data breach will differ on a case-by-case basis. How the response will be managed depends on:

- the sensitivity of the information
- who the information was disclosed to
- what happened to the information once it was disclosed
- how the information was disclosed
- if there was any misconduct involved.

The following provides an overview of the steps involved in responding to a data breach. For more detailed information on how to respond to a data breach refer to the WBHHS Data Breach Response Plan or contact the PCCO WBHHS-Privacy@health.qld.gov.au

Step 1: Containment and mitigation

All employees who identify or are made aware of an actual or suspected data breach must:

- immediately take reasonable steps to contain the data breach to mitigate harm. This may include:
  - recovering or retrieving the lost data
  - suspending activities that led to the data breach
  - isolating or suspending affected systems
  - revoking or changing access codes and passwords
- Report the incident to a line manager and the PCCO WBHHS-Privacy@health.qld.gov.au

Step 2: Assessment

An assessment must be undertaken within 30 days of the data breach to ascertain whether there are reasonable grounds to believe it is an eligible data breach under the MNDB scheme. The details of the breach, the assessment and outcome must be documented for recordkeeping.

Assessments are led by the PCCO and DBRT and will require cooperation from employees and their line managers involved in the data breach.

If the DBRT require more time the PCCO will request an extension from the OIC.

Step 3: Notification

Eligible data breaches, their investigation and outcomes must be prepared as a statement and provided to the OIC. Any affected individuals must be notified in writing. This may include a notification letter to one or more affected individuals and or a published notice on WBHHS and OIC website for a period of at least 12 months.

If another agency is affected by the data breach WBHHS must give written notice to that agency describing the data breach but not including any personal information in the description.

While not required by the IP Act, it may be appropriate to notify other entities of a data breach, for example:

- Australian Digital Health Agency for data breaches involving the My Health Record

- Queensland State Archivist for lost public records containing personal information
- Crime and Corruption Commission Queensland for 'corrupt conduct'
- Queensland Police Service for theft of devices.

Where a notification exemption under the IP Act is applicable, WBHHS will inform the OIC in writing that it is exempt from complying with the obligations outlined in the MNDB scheme.

Notifications are prepared by the DBRT and cleared by the office of the WBHHS CE.

Step 4: Post data breach review and remediation

To mitigate future risks, prevent reoccurrence of similar breaches, and improve personal information handling practices a post response assessment must occur. This includes a strategy to remediate any identified system weaknesses or control deficiencies.

Post data breach reviews and remediation strategies are undertaken by the relevant members of the Data Breach Response Team and reportable to the relevant WBHHS Data Custodians, and the Board, Audit and Risk Committee.

Data Breach Register and Record Keeping

WBHHS maintains a data breach register for recording details about all data breaches, including those that do not meet the definition of an eligible data breach. The data breach register assists with the investigation, reporting and post data breach review and includes:

- a description of the data breach,
- the steps taken to contain and mitigate the breach and its harm.
- actions taken to prevent future data breaches of a similar kind occurring.
- whether the breach is an eligible data breach
- the date the OIC was notified of an eligible data breach
- the names of affected individuals and the date they were notified
- the reason and date an exemption from notification was made to the OIC

All records including emails relating to the assessment and post data breach review are to be retained in accordance with the *Public Records Act 2023* (Qld) and General Retention and Disposal Schedule.

The PCCO is responsible for maintaining the data breach register.

4. Roles and Responsibilities

Role	Responsibility
Employee	Read the WBHHS QPP Privacy Policy, WBHHS Data Breach Policy and WBHHS Data Breach Response Plan and understand what is expected. Comply with the IP Act and QPPs, including protecting personal information held by the agency from unauthorised access, disclosure or loss. Immediately report a data breach or suspected data breach to the line manager and PCCO for further investigation. Respond to requests for information from and cooperate with the PCCO and DBRT. Monitor and manage mandatory training.
Privacy and Confidentiality Contact Officer	Assess all data breaches and determine actions to be taken including determining reasonable suspicion or belief of an eligible data breach. Immediately report a data breach that is also a cyber security incident to the Chief Information Officer, if not already reported. Convene relevant members of the DBRT in the investigation of eligible data breaches.

Role	Responsibility
	Maintain the data breach register and associated records. Prepare data breach notifications to the OIC, affected persons and others where required for clearance through the WBHHS CE Office. Prepare reports to WBHHS data custodians and Board Audit and Risk Committee.
Line Manager and Application/Data Manager	Identify and escalate privacy, information security and cybersecurity concerns within area of responsibility. Immediately report a data breach to the PCCO and if also a cyber security incident, to the Chief Information Officer. Monitor and manage mandatory training. Manage user access to digital systems including SharePoint. Enforce compliance with privacy, information and cyber security policies and procedures.
Data and Application Custodians	Facilitate the review of data breaches and implementation of remediation strategies. Enforce compliance with privacy, information and cyber security policies and procedures.
Data Breach Response Team	Assist in the investigation of data breaches where there is reasonable suspicion or reasonable belief of an eligible data breach. Assist in the preparation of data breach notifications to the OIC, affected persons and others where required for clearance through the WBHHS CE Office. Undertake post data breach reviews and implement remediation strategies.

5. Supporting / Relating documents

- Information Privacy Act 2009 (Qld)
- Hospital and Health Boards Act 2011 (Qld)
- Right to Information Act 2009 (Qld)
- Privacy Act 1988 (Cth)
- Public Health Act 2005 (Qld)
- Mental Health Act 2016
- Public Records Act 2023
- Public Sector Ethics Act 1994 (Qld)
- Human Rights Act 2019 (Qld)
- Security of Critical Infrastructure Act 2018 (Cth)
- Information and cyber security policy (IS18)
- Queensland Health Information Security Policy
- Code of Conduct for the Queensland Public Service
- National Safety and Quality Health Service Standard (NSQHS), Standard 1 – Clinical Governance

6. Definitions

Term	Definition
Affected individual	A person whose personal information is subject to a data breach or eligible data breach
Data breach	The unauthorised access or disclosure of information held by an agency or the loss of personal or non-personal information held by an agency where unauthorised access or disclosure is likely to occur.
Data breach response plan	A more detailed internal procedural document complementing the Data Breach Policy, detailing the more specific processes in managing and responding to a data breach.
Data breach response team	A team consisting of senior WBHHS personnel responsible for coordinating and managing an eligible data breach, post review and remediation strategies.
Eligible data breach	An "Eligible Data Breach" will have occurred under section 47 of the IP Act where: (a) there has been unauthorised access to, or unauthorised disclosure of personal information held by WBHHS, and the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates; or (b) there has been loss of personal information held by WBHHS that is likely to result in unauthorised access to, or unauthorised disclosure of the personal information, and the loss is likely to result in serious harm to any of the individuals to whom the information relates.
Mandatory Notification of Data Breach (MNDB) scheme	A mandatory reporting obligation created under Chapter 3A of the IP Act.
Personal information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: • Whether the information or opinion is true or not; and • Whether the information or opinion is recorded in a material form or not.
Personal information held by WBHHS	Information contained in a document in the possession or under the control of WBHHS. This may include documents stored in IT systems or paper files and can include documents held by contracted service providers.
Office of the Information Commissioner (OIC)	The independent statutory body in Queensland responsible for overseeing the administration of the RTI Act and IP Act, promoting access to information held by Queensland public sector agencies and protecting personal information.
Reasonable belief of an eligible data breach	Sufficient information exists to confirm a data breach is an eligible data breach.
Reasonable suspicion of an eligible data breach	Insufficient information exists to confirm a data breach as an eligible data breach and further investigation maybe required to determine reasonable belief.
Serious harm	Serious physical, psychological, emotional, reputational or financial harm to the individual because of the access or disclosure
Unauthorised access	Access by someone who is not authorised to do so or for a purpose that is not directly related to their duties or work functions. For example, an employee accessing clinical records of a celebrity out of curiosity, or a cybersecurity incident.
Unauthorised disclosure	Intentional or unintentional disclosure of personal information when not authorised to do so. For example, emailing personal information to the wrong recipient, intending to provide deidentified information to a recipient but accidently including identifiers. Unauthorised access and disclosure are not mutually exclusive and can occur because of the same breach or as part of a chain of events

Term	Definition
Loss	No longer having possession or control of the information. Loss may occur because of a deliberate or accidental act or omission, or due to the deliberate action of a third party. For example, disposal of a laptop or filing cabinet that still contains personal information, accidentally leaving a USB or external drive containing personal information on public transport, theft of clinical records or devices containing personal.

7. Policy revision and approval history

Document Executive	Executive Director Finance and Performance				
Document Steward	Director Information Management				
Risk Rating					
Approval Authority	Executive Strategic Management Committee				
Keywords					
Supersedes	Not applicable				
Version	**Approved**	**Effective**	**Authority**	**Comment**	**Review**
V1.0	13/08/2025	13/08/2025	Executive Strategic Management Committee	To provide guidance, visibility to how the HHS manages data breaches.	01/08/2028

Authorised by: Executive Director Finance and Performance

8. Appendices

- **Appendix A:** Examples of Data breaches

Appendix A: Examples of Data breaches

Human Error	**An unintended action by an individual directly resulting in a data breach**
Failure to use Blind Carbon Copy (BCC) when sending email	Sending an email to a group of people and placing all recipient emails addresses in the 'To' field, thereby disclosing all recipient email addresses to all recipients
Failure to appropriately dispose of personal information	Not confidentially destroying personal information after use
Failure to redact personal information	Failure to de-identify and/or delete personal information from a document record before it is disclosed
Failure to use encryption software	Sharing personal information via email without using encryptions software of secure file transfer
Failure to maintain digital system security	Systems security not maintained through the application of known and supported patches
Inappropriate disposal of data storage devices	Computer hard drives and other storage media being disposed of without erasing the contents
Inappropriate sharing of passwords	Sharing passwords with others who may not be authorised to access information systems
Incorrect personal information attached to a client file	Personal information is attached to a client file which is then subsequently accessed or disclosed
Insecure disposal	Disposing of personal information documents in a manner that results in unauthorised loss or disclosure. For example, placing documents in a public bin to dispose of customer records instead of the secure disposal bin
Loss of paperwork, laptop or data storage device	The physical loss of personal information. This may be where an employee accidently leaves a client folder on a train or leaves a work laptop in a taxi
Onforwarding personal information in correspondence	Personal information included in correspondence sharing when the recipient is not authorised to receive the personal information
Personal information sent to the wrong recipient	Personal information sent to the wrong recipient via email, fax, post, courier service or other electronic method including
Unauthorised access	Where personal information is accessed without authority or a purpose that is not directly related to the persons duties or work functions. This includes taking documents containing personal information home or leaving computers accessible.
Unauthorised verbal disclosure	Verbally sharing personal information without authorisation. This may include sharing or openly discussing sensitive medical information in a hospital waiting room, while MS Teams in an open office or while working from home.
Unauthorised disclosure by unintended release or publication	Unauthorised disclosure of personal information in writing, sending a letter to the wrong address, but with the correct name or publishing information online
Malicious or Criminal attack	**A malicious or criminal attack, deliberately crafted to exploit known vulnerabilities for financial or other gain**
Business email compromise	A form of cybercrime that uses email fraud to attack an organisation to achieve a specific outcome that negatively impacts the target organisation
Brute force attack	A typically unsophisticated and exhaustive process to determine a cryptographic key or password that proceeds by systematically trying all alternatives until it discovers the correct one
Compromised or stolen credentials (method unknown)	Credentials are compromised or stolen by methods unknown
Cyber incident	A cyber incident targets computer information systems, infrastructures, computer networks or personal computer devices
Hacking	Unauthorised access to a system or network (other than by way of phishing, brute-force attack, or malware), often to exploit a system's data or manipulate its normal behaviour
Malware	Short for 'malicious software'. Software used to gain unauthorised access to computers, steal information and disrupt or disable networks. Types of malwares include trojans, viruses and worms

Phishing (compromised credentials)	Untargeted, mass messages sent to many people asking for information, encouraging them to open a malicious attachment, or visit a fake website that will ask the user to provide information or download malicious content
Ransomware	Malicious software that makes data or systems unusable until the victim makes a payment
Rogue employee/insider threat	Intentional attack by an employee or insider (e.g. contractor) conducting activities that are not in the interest of the employer or other entity
Social engineering/impersonation	Directed attack that relies heavily on human interaction to manipulate people into breaking normal security procedures and best practices to gain access to systems, networks or physical locations
Theft of paperwork, laptops or data storage device	Theft of a physical device or paperwork containing personal information
System Fault	**A business or technology process error not caused by direct human error**
Mail merge failure	A system failure which results in personal information being misdirected to the incorrect individual
Unintended release or publication	A system failure which results in the release or publication of personal information