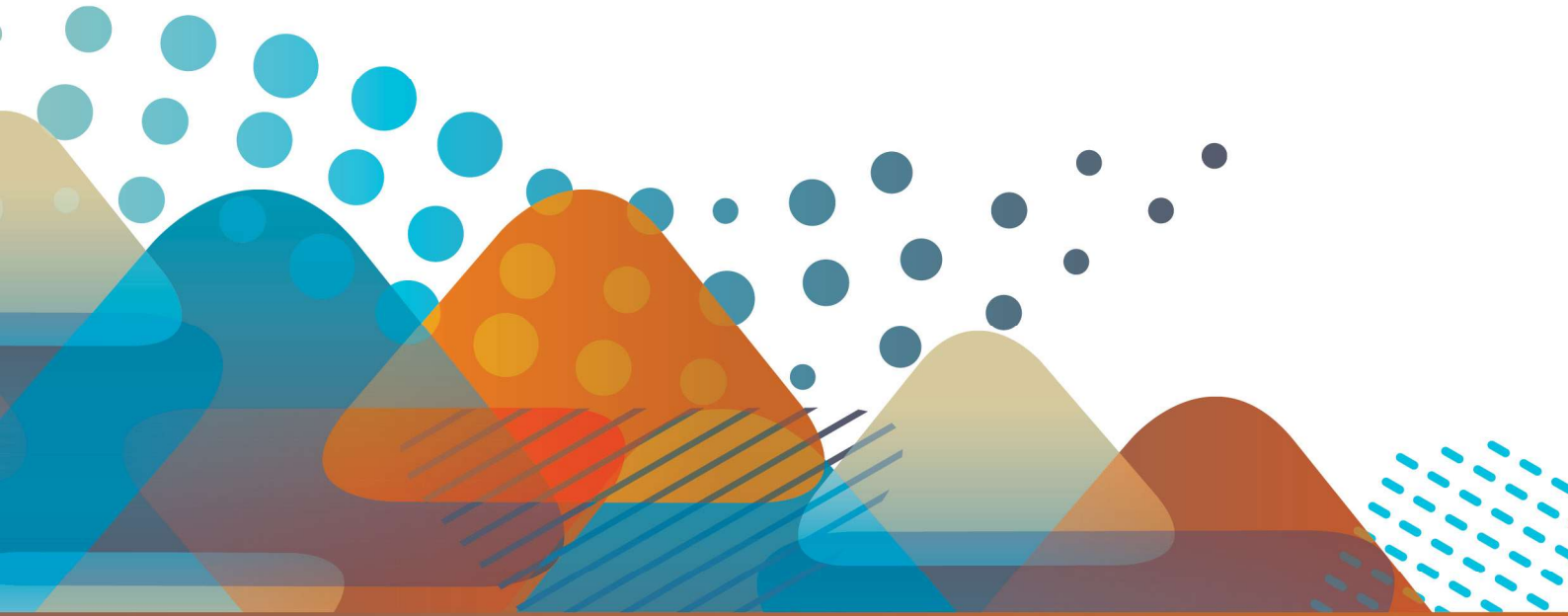
North West
Hospital and Health Service

Privacy Plan

North West Hospital and Health Service



Pathways to better health
for our North West communities

Queensland Government

Contents

Privacy Statement

The North West Hospital and Health Service respects the privacy of patients, their families and it's employees.

The North West Hospital and Health Service is subject to privacy and confidentiality legislation which set the standards for how we collect and hold personal information, including patient information and employee personal information.

1. Purpose

This Privacy Plan outlines the measures implemented by the North West Hospital and Health Service (NWHHS) to ensure the protection and confidentiality of personal, sensitive, and health information of patients, employees, contractors, volunteers, and visitors. It supports compliance with relevant legislation, including the *Information Privacy Act 2009 (Qld)*, the *Hospital and Health Boards Act 2011 (Qld)*.

For identifying information to be managed in accordance with the requirements of the *Information Privacy Act 2009* "personal information" is defined as:

> *"information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."*

This privacy plan reflects recent reforms under the *Information Privacy and Other Legislation Amendment Act (IPOLA Act) 2023 (Qld)*, which strengthen Queensland's privacy framework. The Act introduces a mandatory data breach notification scheme and enhances the rights of individuals to access and correct their personal information. Our Hospital and Health Service is committed to upholding these principles to ensure the protection and responsible handling of personal information for both patients and staff.

2. Scope

This privacy plan applies to all personal information collected, stored, used, or disclosed by the Hospital and Health Service. It covers information relating to **patients, staff, volunteers, contractors, students**, and **members of the public** who interact with the NWHHS. The plan outlines how personal information is managed in accordance with the *Information Privacy Act 2009 (Qld)* and relevant legislation, ensuring the privacy and confidentiality of individuals is maintained across all areas of our operations and service delivery.

3. Personal Information

3.1 The types of personal information we collect

The types of personal information the NWHHS collect depends on the service or function we need it for. We take care to ask you only for what is necessary. Some examples of the personal information collected by the NWHHS are:

Community	**Employees/prospective employees/ contractors/students/volunteers**
Name Contact details	Name Contact details

Community	Employees/prospective employees/ contractors/students/volunteers
Date of birth Signature Photographs that capture your image or other personal information Unique identifying number (such as your Medicare number) Health information; medical, treatment, and diagnostic Test results, x-rays and scans Correspondence and feedback Complaint information Patient Travel information	Signature Photographs that capture your image or other personal information Financial or bank details, including Tax File Number Education history Cultural background, relationship status and family circumstances Correspondence and feedback Complaint information Details of access and correction requests Occupation and employment history Criminal history Recruitment information

The types of Sensitive Information held by NWHHS for patients or employees can include:
Racial or Ethnic Origin: Information about an individual's ancestry, nationality, or cultural background. Political Opinions: Beliefs or opinions related to political matters, ideologies, or political parties. Religious or Philosophical Beliefs: Information about an individual's faith or worldview. Sexual Orientation: An individual's sexual preference or attraction. Criminal Record: Information about an individual's past criminal activity or convictions. Health Information: Details about an individual's physical or mental health, including medical history, diagnoses, or treatment. Genetic Information: Information about an individual's genetic makeup, including DNA. Biometric Information: Unique physical or behavioural characteristics, such as fingerprints or facial recognition data. Professional or Trade Association Membership: Information about an individual's affiliation with a professional body or trade union. Trade Union Membership: Information about an individual's membership in a labour union.

Community	Employees/prospective employees/ contractors/students/volunteers
Membership of a Political Association: Information about an individual's affiliation with a political organization. Membership of a Professional or Trade Association: Information about an individual's affiliation with a professional or trade organization.	

3.2 When do we collect Personal information?

We may collect personal information directly from you or from someone else, including a relative in an emergency. We collect information when you:

- Visit our website (NWHHS)
- Take part in our surveys
- Communicate with us or provide us with feedback
- Visit a health care facility
- Fill in a form (including online and paper forms)
- Apply for a job with us
- Ask us a question or make a complaint
- Request access to, or correction of, your personal information.

3.3 Why do we collect Personal Information?

The NWHHS collects personal information for a range of critical reasons related to patient care, operational needs, legal obligations, and service improvement. Below is a comprehensive list:

Category	Reasons for collecting Personal Information
Provision of Healthcare Services	To assess, diagnose, treat, and manage a patient's health condition. To maintain a complete and accurate medical record. To ensure continuity of care between different healthcare providers.
Legal and Regulatory Compliance	To comply with mandatory reporting requirements (e.g. notifiable diseases, births, deaths). To meet obligations under healthcare legislation such as the *Hospital and Health Boards Act 2011 (Qld)* and *Information Privacy Act 2009 (Qld)*.

	To comply with legal reporting obligations, such as the notification of communicable diseases under the *Public Health Act 2005 (Qld)*. To meet statutory requirements for documenting births, deaths, or significant health events. To manage consent and decision-making in accordance with guardianship and advance health directive laws.
Administrative and Operational Purposes	To manage hospital admissions, discharges, and appointments. To process Medicare, private health insurance, and other health service claims. To communicate with patients, next of kin, and carers regarding treatment plans and hospital services.
Quality Assurance and Improvement	To monitor, assess and improve the quality and safety of healthcare services. To conduct clinical audits and outcome evaluations. To manage and investigate incidents or complaints.
Training and Education	To support the training and supervision of medical, nursing, allied health, and administrative students (with appropriate consent or de-identification). To facilitate staff professional development and skills maintenance.
Research and Public Health	To support ethically approved medical and health research. To contribute to public health monitoring and health policy development (often using de-identified data).
Workplace Health and Safety	To monitor clinical outcomes and improve safety, quality, and performance. To conduct audits, service evaluations, and patient feedback surveys. To investigate incidents, adverse events, and complaints to identify areas for improvement.
Risk, Legal and Insurance Management	To manage clinical and organisational risk. To investigate and respond to insurance claims, legal proceedings, or coronial inquiries. To support indemnity, liability, and professional conduct requirements.

Coordination of Services	To facilitate referrals and care coordination with other Queensland HHSs, community health, mental health, disability services, aged care, and non-government providers.
Consent and Capacity Management	To determine a patient's decision-making capacity and manage legal authorisations.

4. Data Quality and Security

All North West Hospital and Health Service personnel (including employees, students, interns, volunteers, contractors, consultants, Board Members, and managed service providers) are required to comply with all relevant Information Security Controls.

This includes adherence to the Password Management Standard, and the Information Security Classification and Handling Standard, which require that:

- all reasonable steps are taken to ensure personal information is accurate, up to date, and complete; and
- electronic systems are secured through role-based access controls, encryption, audit logging, and regular backups; and
- paper records are stored securely, with access limited to authorised personnel.

5. Data Breach Management

5.1 NWHHS Data Breach Management Policy

The North West Hospital and Health Service maintains policies on Privacy and Confidentiality, and Data Breach Management which are applicable to all staff, to ensure compliance with legislative requirements and best practice standards. All suspected breaches are assessed under the framework of the IP Act.

If a data breach occurs that is likely to result in serious harm to an individual or NWHHS systems, we will notify affected individuals. Serious breaches (Eligible Breaches) are required to be reported to the Office of the Information Commissioner (Qld).

Our response includes promptly containing the breach, assessing the risks, notifying affected individuals, and taking steps to prevent future occurrences.

If you suspect that your personal information has been mishandled by NWHHS (known as a Data Breach under the IP Act), you should contact the NWHHS Privacy Officer immediately.

To lodge a complaint about a data breach with NWHHS, please ensure your submission meets the following requirements:

- your complaint must be in writing;
- include your name and contact details, so we can get back to you;
- make sure the complaint is about your own personal information, not someone else's personal information;
- give specific detail about your concerns/issues with how the NWHHS has handled your personal information.

For NWHHS to respond to your privacy complaint properly and efficiently, you should ensure that it contains sufficient information to enable NWHHS to understand the nature of your complaint, the impact it has had on you and what outcome you are seeking.

Attach copies of any documents you consider may assist the NWHHS to investigate your privacy complaint.

While conducting the investigation, the nature of your privacy complaint and your identity may need to be disclosed to relevant business areas within the NWHHS and third parties. You can advise us that you do not wish for the NWHHS to disclose your identity, however please be aware that this may mean the NWHHS cannot properly investigate and resolve the privacy complaint.

Your privacy complaint should be marked **Private and Confidential** and sent to:

Privacy Officer
Mount Isa Base Hospital
North West Hospital and Health Service
PO Box
Mount Isa Qld 4825

5.2 Responding to your privacy complaint

An acknowledgement letter or email will be sent to you within 5 business days of the receipt of the privacy complaint. To make sure your personal information is protected, we take precautions to verify the identity of complainants. Depending on the nature of your privacy complaint, we may request that you provide sufficient evidence of identity to progress your complaint. If we require further information, we will contact you.

We will then respond within 45 business days outlining our decision and reasons for this decision.

However, if your privacy complaint is complex or requires extensive work and consultation, we may not be able to respond within 45 business days. If this happens, we will notify of the delay in writing.

5.3 Anonymous privacy complaint

We will accept and process anonymous privacy complaints. However, an anonymous privacy complaint may be difficult to manage as we will not be able to request further information and will not be able to provide a response to the complainant.

5.4 Withdraw a privacy complaint

If you wish to withdraw a privacy complaint, it must be in writing. The NWHHS may continue with the assessment if the privacy complaint involves a serious or significant issue that requires further management.

5.5 Further action

If you are not satisfied with the NWHHS response, or have not received a response, and at least 45 business days have passed since the privacy complaint was made in writing to the NWHHS, you can refer the privacy complaint to the Office of the Information Commissioner (OIC) Queensland.

To take your privacy complaint to OIC, it must be made in **writing**, providing details of your privacy complaint and an address so that the OIC can send you correspondence relating to your complaint. You can post or email your complaint to:

Attention: Privacy Team
Office of the Information Commissioner
PO Box 10143
Adelaide Street
BRISBANE QLD 4001

Email: **administration@oic.qld.gov.au**

Alternatively, you may wish to complete the OIC privacy complaint form available on the OIC website (**www.oic.qld.gov.au**) and lodge the completed form online or print out and send the form to the OIC.

Note Before you can submit your complaint to the OIC, you **must** make your privacy complaint to the NWHHS first and wait for the relevant timeframe as outlined in section 5.2.

7. Training and Awareness

- All new NWHHS staff receive induction training on privacy obligations.

- Annual Code of Conduct refresher training is mandatory for NWHHS staff, which includes the requirement to treat official information with care and use it only for the purpose for which it was collected or authorised, to store official information securely, limiting access to those persons requiring it for legitimate purposes and not using confidential or privileged information for further personal interests.
- Targeted education is provided for roles handling sensitive or large volumes of personal information.

8. Key Definitions

Word/Phrase	Definition
Personal Information	Information or an opinion (whether true or not, and whether recorded in a material form or not) about an individual whose identity is apparent or can reasonably be ascertained.
Sensitive Information	A subset of personal information, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious beliefs • Sexual orientation or practices • Health or disability • Criminal record • Membership of a professional or trade association
Health Information	Personal information about the health, disability, or medical history of an individual, including: • Symptoms, diagnosis, treatment, or medication • Health services provided to the individual • Genetic information
Confidential Information	Information that could identify a person receiving, or who has received, a public sector health service. This includes data collected during treatment or care and held by a Hospital and Health Service. *Source: Hospital and Health Boards Act 2011 (Qld), Section 139*
Employee Information	Employment information includes employment history, qualifications, performance, payroll, and leave records for employees.

Privacy Breach	A privacy breach occurs when there is unauthorised access to, disclosure of, or loss of personal information, or failure to protect such information from misuse or interference.
Data Breach	An incident where personal or confidential information is lost or subjected to unauthorised access, disclosure, modification, or destruction. Often overlaps with the term “privacy breach” but is typically used in the context of cybersecurity and breach response.
Information Privacy Principles (IPPs)	A set of principles under the *Information Privacy Act 2009 (Qld)* that public sector agencies must follow when collecting, storing, using, and disclosing personal information.
Right to Information (RTI)	The legal right for individuals to access documents held by government agencies, unless access would be contrary to the public interest. *Source: Right to Information Act 2009 (Qld)*
Information Access Request	A request made under either the *Information Privacy Act 2009 (Qld)* (for personal information) or the *Right to Information Act 2009 (Qld)* (for non-personal or broader information).
Administrative Access	A voluntary, informal process where individuals can access personal or health information without lodging a formal RTI or IP application, where appropriate and feasible.
Privacy Officer	A designated staff member responsible for promoting privacy compliance, managing access requests, coordinating breach responses, and ensuring that policies align with legislation.
De-identified Data	Data that has been stripped of all personal identifiers, and where the risk of re-identification is minimal. De-identified data may be used for reporting, research, or service planning.
Consent	Voluntary agreement by an individual for their personal or health information to be collected, used, or disclosed for specific purposes. Consent should be informed, specific, and current.
Use	The handling of personal information within the agency that collected it. For example, using a patient's contact details to follow up an appointment.
Disclosure	Making personal information available to another entity or person outside the hospital, such as to a specialist, government agency, or insurer.

9. Privacy Legal and Policy Framework

This plan aligns with the following:

- *Information Privacy Act 2009 (Qld)* – including compliance with the Queensland Privacy Principles (QPPs) – See Appendix 1
- *Hospital and Health Boards Act 2011 (Qld)*
- *Information Privacy and Other Legislation Amendment Act (2023)*
- Queensland Health's Information Management and Privacy Policies

10. Privacy Governance and Accountability

Hospital Board / Executive	• Provide strategic leadership and oversight • Approve privacy policies and frameworks	• Ensuring compliance with legislation and risk oversight
Health Service Chief Executive	• Endorse and support the Privacy Plan • Ensure adequate resourcing for privacy and data security	• Overall accountability for privacy compliance
Privacy Officer	• Coordinate privacy policy reviews • Manage access requests and breaches • Provide promotional and educational material about Personal Information security	• Reporting to Executive on privacy matters
Risk & Compliance Committee	• Monitor and review privacy risks, incidents, and compliance • Escalate high-risk issues	• Provide advice to Executive on governance effectiveness
Managers / Supervisors	• Ensure staff comply with privacy protocols • Promote awareness and reporting culture	• Operational responsibility for team compliance
All Staff, Volunteers & Contractors	• Handle personal and health information in accordance with policies	• Individual responsibility under the IP Act and Code of Conduct

	• Report any suspected breaches	
IT / Cybersecurity Team	• Maintain system safeguards and access controls • Investigate digital breaches	• Technical compliance with data security standards
Human Resources	• Ensure employee records are handled lawfully • Educate new staff on privacy obligations	• Workforce privacy compliance
Health Information Services (Medical Records)	• Manage storage, access, and release of health records • Support information access requests	• Accuracy and security of health records
Consumers / Community Members	• Access their personal health information • Provide feedback and raise privacy concerns	• Hold the hospital accountable through rights under the IP and RTI Acts
Office of the Information Commissioner (Qld)	• Oversight authority for RTI/IP Act compliance • Investigate complaints and breaches	• Independent external accountability body

11. Monitoring and Review

- Regular audits are conducted to assess NWHHS compliance with privacy legislation and policies.
- This Privacy Plan, NWHHS Privacy and Confidentiality Policies including the Data Breach Management Policy are reviewed annually or in response to legislative changes or outcomes from reviews of significant incidents.

12. Contact Information

For privacy enquiries or concerns:

Privacy Officer
Phone: 07 47641218
Mount Isa Base Hospital
PO Box 27
Mount Isa Queensland 4825

13. Appendices

13.1 Queensland Privacy Principles

QPP 1 — Open and transparent management of personal information

Requires agencies to manage personal information in an open and transparent way.

Requires a clear, up-to-date and accessible QPP privacy policy, and practices and procedures to ensure QPP compliance.

QPP 2 — Anonymity and pseudonymity

Requires agencies to allow individuals the option of not identifying themselves (i.e. to deal with the agency anonymously or pseudonymously) unless it is:

- required or authorised under law, or
- impracticable.

QPP 3 — Collection of solicited personal information

Provides that agencies:

- can only collect personal information that is reasonably necessary for, or directly related to, one of their functions or activities
- must collect it lawfully and fairly, and
- must collect it from the individual unless an exemption applies (including consent, lawful authority/requirement and law enforcement),or it is unreasonable or impracticable to do so.

Higer standards apply to the collection of sensitive information.

Personal information is only *collected* if the agency solicits it, i.e., they ask someone for it or otherwise takes active steps to acquire it. Unsolicited personal information sent to an agency is not collected and must be assessed under QPP 4.

QPP 4 — Dealing with unsolicited personal information

Requires agencies to assess *unsolicited* personal information to determine whether they could have collected it under QPP 3 and/or whether it is a public record. If not, agencies may be required to destroy or de-identify unsolicited personal information, subject to public record laws. Otherwise, QPPs 5 to 13 apply.

QPP 5 — Notification of the collection of personal information

Requires agencies that collect personal information to take reasonable steps to make sure individuals are aware of the matters listed in QPP 5 including agency contact details, the fact and circumstances of the collection if collected from someone other than the individual and the consequences if the information is not collected.

This applies when personal information is collected from an individual or from a third party.

Agencies do not need to provide a formal QPP 5 notice. The QPP 5 matters can be communicated in other ways, for example, informally or verbally.

QPP 6 — Use or disclosure of personal information

Agencies can only use or disclose personal information for the reason it was collected, unless QPP 6 allows it to be used or disclosed for a secondary purpose. These include:

- instances where the individual has consented to the use of disclosure of the information
- QPP 6 specific secondary purposes, including where:
  - the individual would reasonably expect the agency to use or disclose the information for the secondary purpose (subject to limitations)
  - where it is required or authorised by law or reasonably necessary for law enforcement activities
- permitted general situations such as lessening or preventing a serious threat or locating a missing person (set out in schedule 4, part 1 of the IP Act), and permitted health situations (set out in schedule 4, part 2 of the IP Act).

QPP 10 — Quality of personal information

Requires agencies to take reasonable steps to ensure the personal information:

- they collect, use, or disclose is accurate, up to date, complete, and
- for use or disclosure, is relevant to the purpose of the use or disclosure.

QPP 11 — Security of personal information

Requires agencies to *take reasonable steps to protect* the personal information it holds from

- misuse, interference or loss, and
- unauthorised access, modification or disclosure.

Requires agencies to take reasonable steps to destroy or deidentify personal information that is no longer needed for any purpose and is not a public record or otherwise required to be retained under law or court or tribunal order.

QPP 12, QPP 13 — Access to/correction of personal information

Requires agencies to give access to and correct personal information they hold, subject to limitations.

The following QPP's are not used (i.e. the corresponding Australian Privacy Principles (APPs) were not implemented in the IP Act):

- QPP 7 – Direct marketing
- QPP 8 — Cross-border disclosure of personal information, noting that similar requirements to APP 8 are contained in s.33 of the IP Act
- QPP 9 — Adoption, use or disclosure of government related identifiers.