POLICY

Document ID: WBHHS-POL-2560

Privacy Policy

1. Policy statement

Wide Bay Hospital and Health Service (WBHHS) is committed to ensuring the privacy, security, accuracy and integrity of personal information. This policy explains:

- How WBHHS collects, uses and discloses personal information
- How you can access or amend your personal information
- How you can make a privacy complaint with WBHHS.

2. Scope

This Policy applies 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.

This Policy relates to the personal information collected, used and disclosed in carrying out WBHHS functions and activities and is available to WBHHS and the general public.

3. Guiding Queensland legislation and policies

WBHHS will ensure all personal information is managed in accordance with:

- The *Information Privacy Act 2009* (Qld) (IP Act) and the Queensland Privacy Principles (QPPs) that regulates how WBHHS collects, stores, uses and discloses personal information. The QPPs are described in full in the Information IP Act or in summary at Appendix A of this document.
- Part 7 of the *Hospital and Health Boards Act 2011* (Qld) (HHBA) that regulates the use, disclosure and confidentiality of personal health information
- The Queensland Public Service Code of Conduct, section 4.4, that states employees will:
  - treat official information with care and use it only for the purpose for which it was collected or authorised
  - store official information securely, and limit access to those persons requiring it for legitimate purposes
  - not use confidential or privileged information to further personal interests.
- The Queensland Government Information and Cyber Security Policy (IS18) that ensures Queensland Health applies a consistent, risk-based approach to the implementation of information and cyber security to maintain confidentiality, integrity, and availability.
- The Queensland Health Information Security Policy in line with IS18, that supports WBHHS to implement an Information Security Management System (ISMS); a structured approach to managing sensitive information, mitigate risks and embed cyber resilience.
- Public Records Act 2023 (Qld) that provides a framework for making, managing and accessing public records including those that contain personal information or present and future use.

3.1 Definition of terms

This policy describes information as:

- personal information
- sensitive personal information
- health information

Personal Information

The IP Act provides that personal information is information or an opinion about a living identified individual, or an individual who is reasonably identifiable:

a. whether the information or opinion is true or not; and
b. whether the information or opinion is recorded in material form or not

The individual does not need to be directly identified in the information for it be personal information. It is sufficient if they can reasonably be identified in reference to other information. For example, a patient who is not directly named can reasonably be identified if they have a unique condition and reside in a small geographical location.

For examples of personal information refer to Appendix B.

***Note*:** Although deceased patient information does not come under the IP Act definition, it is still confidential health information and must be used and handled in accordance with the Code of Conduct and HHBA.

Sensitive Personal Information

Sensitive personal information is a subset of personal information and includes health information and other information such as race, religious beliefs, sexual orientation and criminal records.

For further examples of sensitive information refer to Appendix B.

Health Information

Health information is a category of sensitive information collected by WBHHS and can include the following:

- the patient's health status or disability at any time
- the patient's expressed wishes about the future provision of health services
- a health service that has been provided, or that is to be provided, to the patient
- personal information about the patient collected for the purpose of providing, or in providing, a health service
- personal information about the patient collected for donation, or intended donation of their body parts, organs, or body substances.

For further examples of health information refer to Appendix B.

3.2 Collection, use and disclosure of personal information

The WBHHS collects, uses and discloses your personal information to carry out functions and activities which include:

- provision of health services to improve your health and wellbeing.
- communicating with you and receiving your feedback.
- research activities to improve health care practices
- human resources management and recruitment

- security and safety management
- financial management
- legal matters

Personal information is managed in an open and transparent way by providing access to policies and procedures that relate to information privacy.

WBHHS will take reasonable steps to ensure you are generally aware of the reasons personal information is being collected. This extends to third parties providing personal information on your behalf.

Notification of collection may be done verbally, evidenced in the title of a form or via collection notices such as pamphlets, telephone scripts, notice boards, or websites.

Dealing with WBHHS anonymously or using a pseudonym

When dealing with or receiving services from WBHHS there are circumstances in which you can remain anonymous or use a pseudonym (fictitious name) such as making complaints, however this is not the case where:

- required or authorised by law, for example, when applying for a job.
- impractical to do so, i.e. a service cannot be performed without a form of identity

In most instances total anonymity in a health service is not practical.

Collection of personal information

WBHHS solicits personal information from patients, consumers, suppliers, business partners and employees. The personal information may be in a physical or digital format including photography and video media.

WBHHS will:

- only collect the relevant personal information to provide a service or complete an activity
- collect, personal information lawfully and fairly
- collect information from you unless you consent to a third party, it is authorised by law to do otherwise, or it is impracticable to collect it from you.

Refer to Appendix B for examples of the types of person information collected.

WBHHS may also receive unsolicited personal information and will confidentially dispose of the information unless

- It requires an action by WBHHS, for example a complaint or compliment
- It has relevance to WBHHS functions and activities, for example promotion letter introducing a new healthcare service
- It is unlawful to do so, i.e. it contains personal information that must be retained by law.

Use and disclose of personal information

WBHHS uses your personal information for the purposes for which it was given, or for purposes which are directly related to one of our functions or activities. We may also use or disclose personal information for secondary or alternative purposes as permitted under the IP Act. Otherwise, WBHHS does not give your personal information to other government agencies, organisations, or anyone else unless one of the following circumstances applies:

- you have consented
- you would reasonably expect, or have been told, that information of that kind is usually passed to those individuals, bodies, or agencies
- it is otherwise required or authorised by law
- it will prevent or lessen a serious and imminent threat to somebody's life or health

Your personal information may be used for the following activities, noting this is not an exhaustive list:

- providing health care to you including communicating with you, your carers and external health care providers
- conducting research and clinical reviews to improve health outcomes
- conducting surveys about health issues, service quality or satisfaction
- investigating complaints and medicolegal claims
- undertaking recruitment and managing employees and volunteers within WBHHS
- managing and engaging with contracted service providers and third-party suppliers
- managing, funding and monitoring service performance across WBHHS

Service providers or third-party suppliers accessing or dealing with personal information

WBHHS will use contracted service providers and third-party supplier to provide certain services and functions for us. Some examples include:

- outsourced clinical services
- cloud-based storage
- surveys and feedback collation
- diagnostic imaging services
- corporate and clinical record storage

To provide these services and functions, service providers and third-party suppliers may collect and use your personal information on our behalf. To comply with the IP Act and QPPs, WBHHS ensures that service providers and third-party suppliers are contractually bound to meet our obligations through privacy and confidentiality clauses.

When considering the use of service providers and third-party suppliers that will collect and use personal information, WBHHS will complete a Privacy Impact Assessment (PIA) to assess compliance with the QPPs and identify and address potential risks.

Disclosure outside of Australia

WBHHS will only transfer personal information outside of Australia in certain circumstances, such as:

- when you have agreed/consented
- the transfer is authorised or required under a law
- WBHHS is reasonably satisfied that the transfer is necessary to lessen or prevent a serious threat to the life, health, safety, or welfare of any individual, or to public health, safety and welfare
- if two or more of the following apply:
  - the recipient is subject to equivalent privacy obligations
  - the disclosure is necessary to perform a function of WBHHS
  - the disclosure is for your benefit
  - reasonable steps have been taken by the WBHHS to ensure the information is protected.

Instances where WBHHS may transfer personal information outside of Australia include:

- where you have requested us to correspond with you using a web-based email service whose servers are based in another country (e.g., Hotmail or Gmail).
- you have been injured while overseas and your care providers needs your medical history
- you have consented for us to provide your personal information to an overseas insurer.

Personal information and CCTV footage

Some WBHHS locations are equipped with Closed Circuit Television (CCTV) cameras which are used to monitor safety and access, as well as to deter (and capture evidence of) unlawful behaviour. Notices advising of CCTV surveillance are visible at the entry of each facility.

In accordance with the *Public Health Act 2005*, Fire Safety and Security Officers within WBHHS may also be equipped with Body Worn Cameras (BWC) and may record footage when undertaking specific duties relating to the safety of staff, patients and visitors. Staff using a BWC will, where possible, advise you when they are recording.

The CCTV and BWC used are owned by the WBHHS, and footage are generally stored for 30 days for CCTV and 90 days for BWC before it is destroyed.

Access to all digital surveillance material is restricted to its prescribed purpose and may be provided to law enforcement agencies or other regulatory bodies where we are legally required or permitted to.

Personal information and social media

WBHHS maintains several social media accounts for sharing information about our services, general health and wellbeing advice and important health alerts. Personal information that you post on any social medial site becomes captured by that social medial platform's privacy policy. You may instead choose to contact us directly.

3.3 Management of personal information

WBHHS manages your personal information by taking reasonable steps to protect it from misuse, interference, loss, and unauthorised access. This includes, implementing and monitoring a range of information security measures that must meet the requirements of the Queensland government Information and cyber security policy (IS18). These measures are dependent upon the sensitivity or classification level of the personal information and include:

- physical – e.g. physical barriers, locks, swipe cards.
- electronic – e.g. multi-factor authentication, encryption, computer screen time out, network firewalls
- operational – e.g. User access management, training, ID badges

Secure transmission of personal information

WBHHS uses a variety of media to transmit personal information internally and externally such as Queensland Health approved email accounts, secure networked drives, licensed Microsoft cloud-based tools, telephone, or registered mail.

Email transfer of personal information is made secure using encryption, document password protection or secure file transfer services.

Quality assurance of personal information

WBHHS will ensure the personal information it collects, uses or discloses is accurate, complete and up to date. Quality management of personal information includes but is not limited to:

- governance via the information management framework and data quality framework
- updating your personal information that may change over time at each encounter with a WBHHS
- correction and amendment of personal information when requested by you.

Retention and destruction of personal information

Once records (physical and digital) containing your personal information are no longer needed, WBHHS will retain them for the minimum period set out in the relevant Queensland State Archive retention and disposal schedule such as the:

- General Retention and Disposal Schedule
- Health Sector (Corporate Records) Retention and Disposal Schedule
- Health Sector (Clinical Records) Retention and Disposal Schedule

At the conclusion of the minimum retention period records are confidentially destroyed via contracted confidential waste services.

3.4 Access to or amendment of personal information

WBHHS supports your right to apply for access to or correction of your personal information. Requests to access personal information are permitted and considered against relevant legislation and other release mechanisms such as administrative access. Refer to appendix C for contact details.

WBHHS will take reasonable steps to correct personal information where it is satisfied that the information is incorrect. This can be done administratively through face-to-face contact with you or via telephone, online portal or form.

Where WBHHS is not satisfied that the personal information is incorrect, or amending it would breach legislative obligations, or there are no reasonable steps that can be taken to correct it, a notation can be placed against or associated with the personal information in question. These requests are managed more formally through an RTI application. Refer to Appendix C for contact details for making amendments to personal information.

3.5 Making a privacy complaint

WBHHS takes breaches of privacy very seriously. Complaints regarding allegations of breaches of privacy are dealt with in accordance with the WBHHS Privacy Breach Policy and Privacy Breach Plan. Complainants are encouraged to direct their enquiries and concerns to the Privacy and Confidentiality Contact Officer (PCCO) in the first instance via WBHHS-Privacy@health.qld.gov.au.

4 Related Policies

- N/A

5 Related Standards

- *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 Policy revision and approval history

Document Executive	Executive Director Finance and Performance				
Document Steward	Manager Information Management				
Risk Rating					
Approval Authority	Executive Strategic Management Committee				
Keywords	Privacy, Person, Information				
Supersedes	Not applicable				
Version	**Approved**	**Effective**	**Authority**	**Comment**	**Review**
1.0	13/08/2025	13/08/2025	Executive Strategic Management Committee	[Reason / Incident ID]	

Authorised by: Executive Director Finance and Performance

7 Appendices

- **Appendix A:** Queensland privacy principles in brief
- **Appendix B:** Examples of personal, sensitive and confidential health information collected by WBHHS
- **Appendix C:** How to contact WBHHS

Appendix A: Queensland privacy principles in brief

QPP 1 **Open and transparent management of personal information**	Manage personal information in an open and transparent way via up-to-date and accessible privacy policy.
QPP 2 **Anonymity and pseudonymity.**	Allow individuals the option of not identifying themselves unless it is required or authorised under law, or impracticable.
QPP 3 **Collection of solicited personal information.**	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 • 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. Higher 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.**	Assess unsolicited personal information to determine whether it could have collected it under QPP 3 and/or whether it is a public record. If not, agencies may be required to destroy or deidentify unsolicited personal information, subject to public record laws. Otherwise, QPPs 5 to 13 apply.
QPP 5 **Notification of the collection of personal information**	When collecting personal information, agencies are required to take reasonable steps to make sure individuals are aware of the matters listed in QPP 5.2 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 o permitted health situations (set out in schedule 4, part 2 of the IP Act).
QPP 10 **Quality of personal information**	Agencies are required 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**	Queensland Privacy Principles in brief Agencies are required to take reasonable steps to protect the personal information it holds from: • misuse, interference or loss, and • unauthorised access, modification or disclosure. Agencies are required 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.
QPPs 12 and 13 **Access to/correction of personal information**	Agencies are required to give access to and correct personal information they hold, subject to limitations

Appendix B: Examples of personal, sensitive and confidential health information collected by WBHHS

Personal information	Sensitive information	Health information
• name • contact details • date of birth • signature • photographs • unique physical characteristics (e.g. tattoos, birthmarks) • fingerprint or other 'biometrics' • driver's licence number • financial/bank details • educational history • unique identifying number • medical/health/diagnostic information • cultural background, relationship details and family circumstances • details of office bearers in funded organisations (i.e. names) • disability funding and service provision • complaints and investigations • personal information recorded by way of camera surveillance systems (CCTV) • occupation and employment history • criminal history • recruitment information.	• race or ethnic origin • political opinions • membership of a political association • religious beliefs or associations • philosophical beliefs • membership of a professional or trade association • membership of a trade union • sexual preferences or practices • criminal records. • health information	• details about a person's health at any time (e.g. that a person is 'off work sick today'). • a disability of a person at any time (e.g. short-term disability following a stroke). • a person's express wishes about future health services to be provided to them (e.g. a 'do not resuscitate' request). • a health service that has been, is being, or will be provided to a person (e.g. patient treatment plan). • personal information collected about a person for the purpose of, or while providing a health service (e.g. diagnostic tests). • personal information collected in connection with the donation, or intended donation, by the person of their body parts, organs or body substances (e.g. blood or urine samples).

Appendix C: How to contact WBHHS

1. **General requests and enquiries**

   Visit the Wide Bay Hospital and Health Service, website and scroll down to 'contact us' for options to log feedback.

2. **Privacy related requests and enquires**

   Contact the WBHHS Privacy and Confidentiality Contact Officer via WBHHS-Privacy@health.qld.gov.au

3. **Requests and enquiries to access or amend personal information**

   For Bundaberg and Rural Hospitals contact

   Senior Information Access Officer Bundaberg Hospital

   PO Box 34 Bundaberg Qld 4670

   Phone: (07) 4150 2124

   Email: WBHHS-IAU@health.qld.gov.au

   For Maryborough and Hervey Bay Hospitals contact:

   Legal Services Officer

   PO Box 592 Pialba Qld 4655

   Phone: (07) 2100 9997

   Email: WBHHS-RTI@health.qld.gov.au