

Townsville Hospital and Health Service

Privacy and Data Breach Management Policy

THHSCOR161077v3

Table of Contents

Policy Overview	3
Intent of this Policy	3
Scope	3
General Information.....	3
What personal information do we collect?	3
Personal Information	3
Sensitive Information.....	4
Confidential Information	4
How do we use and share personal information?	4
Use and disclosure of Personal Information	4
Disclosure outside of Australia	5
How do we manage personal information?	5
Security of personal Information.....	5
Social media and digital images.....	5
Privacy of images and recordings	5
Use of recording devices by visitors.....	5
How to access or correct your personal information?	6
Anonymity or pseudonymity.....	6
How we manage data breaches	6
Responding to a data breach	6
Contain and mitigate	7
Assessment.....	7
Notification.....	7
Review and evaluate	8
How you can make a privacy complaint	8
Privacy Complaint to us.....	8
Privacy Complaint to Office of the Information Commissioner.....	8
Definitions	9

Policy Overview

Townsville Hospital and Health Service (HHS) is committed to protecting the privacy and confidentiality of the personal, sensitive and confidential information that is collected, used, held and disclosed.

Townsville HHS manages the collection, use, storage, disclosure, access, security and quality of personal, sensitive and confidential information, in accordance with the *Information Privacy Act 2009* (Qld) and Part 7 of the *Hospital and Health Boards Act 2011* (Qld).

Intent of this Policy

This policy describes:

- The types of personal information Townsville HHS collects and holds, how that personal information is collected and held, and the purposes for which that personal information is collected, held, used and disclosed
- How Townsville HHS will respond to data breaches including suspected eligible data breaches.
- How to make a complaint about the Townsville HHS's handling of personal information and how Townsville HHS deals with complaints.

Scope

This policy applies to all Townsville HHS employees and any volunteers, contracted service providers, consultants (including Visiting Medical Officers), students and persons or organisations authorised to administer, develop, manage and support Townsville HHS information systems and assets. It also applies to patients, visitors, carers and consumers entering our health facilities.

General Information

The *Information Privacy Act 2009* (Qld) (**IP Act**) provides for the fair collection and handling of personal information in the public sector environment. The Queensland Privacy Principles (**QPPs**) set rules for public sector agencies, such as Townsville HHS about the collection, use, quality, security and disclosure of personal information. Townsville HHS must take reasonable steps to ensure personal information is protected from unauthorised access, use, disclosure, loss, destruction and other misuse, respond to suspected data breaches, and report eligible data breaches as set out in the IP Act.

What personal information do we collect?

Personal Information

Personal information is information about a person who is identified, or can reasonably be identified. Personal information:

- ❖ can be factual information or an opinion about someone
- ❖ can be correct or incorrect
- ❖ can be written, electronic, verbal, visual, or in another form
- ❖ includes information that could identify a person on its own or when combined with other information.

Personal information may be in any form, such as in correspondence, databases, audio recordings, images, alpha-numerical identifiers, CCTV or social media. Examples of personal information held by Townsville HHS are:

Consumers:	Employees / prospective employees/ contractors / students / volunteers
• Name • Contact details • Date of Birth • Signature • Ethnicity • Photographs that capture your image or other personal information • Unique identifying number (such as your Medicare number, health fund details) • Health information • Correspondence and feedback • Complaint information • Patient travel information	• Signature • Identification photographs • Financial or bank details, including Tax File Number • Education history, occupation, employment and recruitment history • Cultural background • Criminal history • Recruitment information
• Camera surveillance (CCTV) footage or body-worn camera (BWC) footage	

Townsville HHS collects and holds personal information required to deliver public sector hospital services and undertake its functions, including health services, teaching, research and other services.

Personal information is usually obtained directly from the individual that the information is about, however may be obtained from third parties in certain circumstances, e.g. another hospital, next of kin, treating general practitioner or legal guardian.

Sensitive Information

Sensitive information is a subset of personal information. Townsville HHS must not collect sensitive information about an individual except in providing health services, and either the collection is required or authorised by Australian law, or the individual would reasonably expect collection of sensitive information for that purpose.

Confidential Information

Confidential information is information about a person who is receiving or has received a public health service. Townsville HHS employees are bound by a strict duty of confidentiality not to disclose confidential information, except where required or permitted under the HHB Act.

How do we use and share personal information?

Use and disclosure of Personal Information

Townsville HHS uses and discloses personal information only where:

- It is for the primary purpose for which it was collected
- The individual would expect the information to be used or disclosed
- The individual has consented
- It is necessary for approved research relevant to public health or safety
- It is reasonably believed disclosure is to prevent harm to the individual or the public

- It is reasonably believed disclosure is necessary to investigate unlawful activity
- It is authorised or required by law.

Disclosure outside of Australia

Townsville HHS prefers not to disclose personal information outside of Australia, however there are occasions where Townsville HHS does disclose personal information outside of Australia. These disclosures are carefully considered and meet requirements of the IP Act.

The IP Act permits disclosure outside of Australia if:

- The individual has agreed; or
- The disclosure is authorised or required by law; or
- Townsville HHS is satisfied, on reasonable grounds, that the disclosure is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of the individual, or to public health, safety and welfare; or
- If two or more of the criteria below apply:
 - The recipient is subject to equivalent privacy obligations
 - The disclosure is necessary to perform a function of Townsville HHS
 - The disclosure is for the individual's benefit, but it is not practicable to seek the agreement of the individual, or the individual would be likely to give the agreement
 - Reasonable steps have been taken to ensure the information is protected.

How do we manage personal information?

Security of personal Information

Townsville HHS holds personal information securely and takes reasonable steps to protect it from misuse, interference, loss, unauthorised access, modification and unauthorised disclosure. Townsville HHS complies with the Queensland Government Information and Cyber Security Policy (IS18) and the Queensland Government Information Security Classification Framework (QGISCF).

Where permitted by the *Public Records Act 2023 (Qld)*, Townsville HHS will destroy or deidentify personal information that has reached its retention period under the relevant Retention and Disposal Schedule, or if the personal information is unsolicited and it is no longer required for any Townsville HHS functions.

Social media and digital images

Information about individuals will never be posted on social media sites, unless through authorised public relations officers on the official Townsville HHS social media pages and print media, and with consent.

Privacy of images and recordings

The capture of images and recordings only occurs when it is necessary for functions or activities relating to the delivery or management of health care services, or through public relations authorised media with consent.

Use of recording devices by visitors and patients

Visitors and patients to Townsville HHS may wish to use recording devices to take photographs, film or make audio recordings. In some situations, this is not appropriate or permitted due to potential invasion of privacy and confidentiality of fellow patients, employees and visitors.

Use of personal recording devices within Townsville HHS facilities is to be considered on a case-by-case basis in consultation with employees, patients and family/carers. There can be situations where it is appropriate and useful for recordings to take place for private purposes, with the consent of all relevant parties¹. Where consent of all parties is not obtained, the recording cannot proceed.

How to access or correct your personal information?

Individuals can apply for access or amendment to their personal information that is held by Townsville HHS. Requests for information can be sent to TSV-TTH-ROI@health.qld.gov.au. Further information is available at: [How do I access information? | Townsville Hospital and Health Service](#).

Anonymity or pseudonymity

Individuals have the option of dealing with Townsville HHS anonymously or using a pseudonym. Townsville HHS supports individuals dealing with us anonymously or under a pseudonym in some circumstances, for example, when making a complaint. Individuals need to consider the following impacts if deciding to deal with us anonymously or under a pseudonym:

- An individual's full clinical record may not be able to be provided to clinical staff to obtain a holistic view of past medical history/treatments
- Inability to contact the individual about their health situation or their complaint
- Limitation to access and correction of personal information as this can only be achieved where individuals provide identification.

How we manage data breaches

A data breach is an eligible data breach if the unauthorised access, unauthorised disclosure or loss is likely to result in serious harm to an individual to whom the personal information relates.

A data breach occurs if there is:

- Unauthorised access to, or unauthorised disclosure of, personal information; or
- Loss of personal information in circumstances where unauthorised access to, or unauthorised disclosure of, personal information is likely to occur.

Townsville HHS strives to ensure security of all personal information and prevent data breaches. If a data breach does occur, Townsville HHS will meet its obligations under the IP Act to ensure that eligible data breaches are contained and any harm is mitigated. Townsville HHS takes reasonable steps to notify a person affected by an eligible data breach, as well as the Office of the Information Commissioner (the Information Commissioner), as soon as possible but within 30 days, unless it is exempt from making such notifications. This will include notifying the person affected of what the Townsville HHS is doing to contain the data breach and any steps that the person should take in response to the data breach.

Responding to a data breach

A data breach may be identified by Townsville HHS:

- By proactive monitoring of system access and use
- An employee identifying an incident

¹ Section 227A of the Criminal Code makes it an offence to video record people without their consent in places where they would expect to be private. Examples such as a bedroom, bathroom, treatment space, staffroom or changeroom.

- Identification of a cyber security breach via monitoring activities and alert notifications
- A member of the public making a complaint to Townsville HHS that a data breach may have occurred.

If it is reasonably suspected that an eligible data breach has occurred, the Information Privacy Officer will convene a Data Breach Response Group within one business day to coordinate and direct the Townsville HHS response, including containment and mitigation strategies, assessment of the data breach and notifications. The Data Breach Response Group consists of:

- Executive Director Digital Health and Knowledge
- Director Clinical Information Management
- Information Privacy Officer
- Director Information Technology Services (as required)
- Director Legal Services
- Director Media, Communications and Engagement
- Service Group Director or Professional Lead (as required)
- Director Human Resources Services (as required)
- Relevant business unit
- eHealth Queensland (as required).

Townsville HHS maintains a register of eligible data breaches to record steps taken in response and management of the data breach.

Contain and mitigate

Upon identification of a data breach, Townsville HHS will take immediate steps to contain the breach and mitigate any harm that may be caused by the breach. The Data Breach Response Group will oversee containment and mitigation activities and may direct further containment and mitigation actions.

Assessment

Within 30 days, the Data Breach Response Group will assess the data breach to determine if it meets the threshold of an eligible data breach. In making an assessment, the Data Breach Response Group will consider the kind and sensitivity of personal information accessed, disclosed or lost, the nature of the harm likely to result from the data breach, and other relevant matters.

Notification

If a data breach is assessed as an eligible data breach, unless an exemption applies, Townsville HHS must notify:

- The Information Commissioner, as soon as practicable
- Affected individuals, as soon as practicable, unless it is reasonably believed that notification will create a serious risk of harm to an individual's health or safety, or if the notification is likely to compromise or worsen cyber security or lead to further data breaches
- Office of the Health Ombudsman (where relevant)
- Crime and Corruption Commission (where relevant)
- Queensland Police Services (where relevant).

Where it is reasonably practicable, Townsville HHS will always take reasonable steps to notify each individual whose personal information has been accessed, disclosed or lost, however if it is not reasonably practicable to do so, then the Townsville HHS will publish a notification on the Townsville HHS website for a period of 12 months.

Review and evaluate

The Information Privacy Officer, in consultation with the Data Breach Response Group, will conduct a post-breach review and evaluation of the eligible data breach response to identify opportunities for improvement.

How you can make a privacy complaint

Privacy Complaint to us

If you have concerns about how Townsville HHS has handled your personal information, you can make a privacy complaint in one of the following ways:

Website: [Feedback | Townsville Hospital and Health Service](#)

Email: THHS_Privacy_and_Confidentiality@health.qld.gov.au

Townsville HHS has 45 business days after the day the privacy complaint is received to respond to the complaint, unless it is otherwise agreed by you to a further specified period.

Privacy Complaint to Office of the Information Commissioner

If you are not satisfied with the outcome of your privacy complaint to us, you also have the option to lodge your privacy complaint to the Office of the Information Commissioner (OIC). Your complaint to the OIC must be in writing, provide details about your privacy complaint and provide an address so they can send you correspondence relating to your complaint. A complaint can be lodged with the OIC in one of the following ways:

Website: [How to make a privacy complaint | OIC](#)

Email: administration@oic.qld.gov.au

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

Definitions

Term	Definition	Source
Confidential information	Confidential information means – a) Information, acquired by a person in the person's capacity as a designated person, from which a person who is receiving or has received a public sector health service could be identified; or b) Information accessed by a prescribed health professional under section 161C(2).	<i>Hospital and Health Boards Act 2011 (Qld)</i>
Data breach	A data breach, of an agency, means either of the following in relation to information held by the 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.	<i>Information Privacy Act 2009 (Qld)</i>
Eligible data breach	1) An eligible data breach of an agency is a data breach of the agency that occurs in relation to personal information held by the agency if – a) Both of the following apply – i) The data breach involves unauthorised access to, or unauthorised disclosure of, the personal information; ii) The access or disclosure is likely to result in serious harm to an individual (an affected individual) to whom the personal information relates, having regard to the matters stated in subsection (2); or b) The data breach involves the personal information being lost in circumstances where – i) Unauthorised access to, or unauthorised disclosure of, the personal information is likely to occur; and ii) If the unauthorised access to or unauthorised disclosure of the personal information were to occur, it would be likely to result in serious harm to an individual (also an affected individual) to whom the personal information relates, having regard to the matters stated in subsection (2). 2) For subsection (1)(a)(ii) and (b)(ii), the matters are – a) The kind of personal information accessed, disclosed or lost; and b) The sensitivity of the personal information; and c) Whether the personal information is protected by 1 or more security measures; and d) If the personal information is protected by 1 or more security measures – the likelihood that any of those security measures could be overcome; and e) The persons, or the kinds of persons, who have obtained, or who could obtain, the personal information; and f) The nature of the harm likely to result from the data breach; and g) Any other relevant matter.	<i>Information Privacy Act 2009 (Qld)</i>

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 – a) Whether the information or opinion is true or not; and b) Whether the information or opinion is recorded in material form or not.	<u>Information Privacy Act 2009 (Qld)</u>
Sensitive information	Sensitive information, for an individual, means the following – a) Information or an opinion, that is also personal information, about the individual's – i. Racial or ethnic origin; or ii. Political opinions; or iii. Membership of a political association; or iv. Religious beliefs or affiliations; or v. Philosophical beliefs; or vi. Membership of a professional or trade association; or vii. Membership of a trade union; or viii. Sexual orientation or practices; or ix. Criminal record; b) Health information about the individual; c) Genetic information about the individual that is not otherwise health information; d) Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or e) Biometric templates.	<u>Information Privacy Act 2009 (Qld)</u>
Serious harm	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.	<u>Information Privacy Act 2009 (Qld)</u>