Standard 1 Governance for Safety and Quality in Health Service Organisations

Policy

TCHHS-QSR-POL-1248

Privacy and confidentiality of personal information

1. Policy statement

The Torres and Cape Hospital and Health Service (TCHHS) are required by law to maintain confidentiality of personal information which includes personal information of patients, consumers and employees. TCHHS is committed to developing a culture of privacy that values personal information, sensitive personal information and confidentiality.

Protecting client personal information and sensitive personal information is important to ensure health care providers have accurate information upon which to correctly assess, diagnose and care for individuals.

Protecting staff personal information and sensitive personal information is important to ensure employment provisions can be adequately provided to staff.

Maintaining confidentiality of personal information and sensitive personal information is paramount to ensuring a trusting relationship between the individual, the health service and between each other.

2. Scope

Applies to all

- TCHHS permanent, temporary, and casual employees
- Visiting Medical Officers, other partners, contractors, consultants, students, trainees and volunteers.
- Business owners/ information asset custodians, administrators and line managers have an explicit need to understand the requirements set by this policy.

3. Definitions

3.1.1. Personal information

Personal information is 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. Section 12 Information Privacy Act 2009

Examples include:

- A person's name, address, phone number or email address
- A photograph of a person, a video recording of a person, image on Closed-circuit television (CCTV).

3.1.2. Sensitive personal information

Sensitive personal information is a subset of personal information and it is important because of the heightened meaning or value to the individual concerned (Information Privacy Act 2009 Schedule 5 Dictionary).

Examples include:

- Racial or ethnic origin
- Sexual preferences or practices
- Political opinions, religious beliefs or associations
- Health information about an individual for the National Privacy Principals.

3.1.3. Health information

Health information is a combination of personal information and sensitive personal information that includes any of the following:

- An individual's health including a disability at any time
- A health service that has been provided, or that is to be provided, to the individual
- Personal information about an individual collected in order to provide, or in providing, a health service.

3.1.4. Confidential information

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 (section 139 Definitions for Part 7 Hospital and Health Boards Act 2011).

3.1.5. Privacy

In the context of privacy principles, privacy is the right that personal information (who we are, what we do, what we think, what we believe) will be protected and there is a right to apply to amend it if it is not accurate, complete or is misleading.

3.1.6. Confidentiality

Confidentiality is the act of not disclosing personal information without authority, i.e., keeping personal information private or in confidence.

3.1.7. Privacy breach

A privacy breach occurs when there is a failure to comply with one or more of the privacy principles set out in the *Information Privacy Act 2009*. A privacy breach most commonly, but not exclusively, results in unauthorised access to, or the unauthorised collection, use, or disclosure of, personal information.

4. Principles

4.1 Collection of personal information

- The TCHHS will only collect personal information that is necessary for its functions or activities (including provision of health care services), and will do so lawfully, fairly and without unnecessary intrusion.
- Information should be sourced from the person about whom the information pertains; however this may depend on the situation, such as whether the individual is capable of providing information at the time.
- The TCHHS will notify a person about what information is being collected, why (including whether there is a lawful requirement) and what the TCHHS intends to do with it.

4.2 Limits on use or disclosure of personal information

- The TCHHS will use and disclose personal information in accordance with laws and policy.
- The TCHHS will use personal information in a way to ensure confidentiality is maintained.
- The TCHHS will ensure personal information of a patient/ client is only made available to a person, authority or other staff member where they are immediately responsible for the health care of a person.
- The TCHHS will ensure personal information of a staff member is only made available to a person, authority or other staff member where they are immediately responsible for the human resource management of the employee.
- The TCHHS will take all reasonable steps to ensure that a contracted service provider complies with the privacy and confidentiality principles.

4.3 Data quality

- The TCHHS will take reasonable steps to ensure that the personal information it collects uses or discloses is accurate and complete when collected.

4.4 Data security

- The TCHHS will take reasonable steps to protect the personal information it holds from misuse, loss and unauthorised access, modification or disclosure.
- The TCHHS will take all reasonable steps to ensure that a contracted service provider is required to comply with the privacy principles and confidentiality and disclosure laws including audit provisions as part of the service contract.
- The TCHHS will ensure personal information is not retained longer than required, e.g., records disposal in accordance with the Public Records Act 2002.

4.5 Openness

- The TCHHS will have policy and procedures for accessing and amending personal information, managing breaches and for making a privacy complaint.
- The TCHHS will publish policies for managing personal information via the TCHHS Publication Scheme.
- The TCHHS will use collection (privacy) notices and will take other reasonable steps to let a person know, generally, what sort of personal information it holds, for what purposes, how it collects, holds, uses and discloses that information.

4.6 Access to documents containing personal information

- The TCHHS will support an individual's general right of access to their own personal information.

4.7 Amendment of documents containing personal information

- The TCHHS will take all reasonable and lawful steps, including making of an appropriate amendment, to ensure the personal information in its custody is accurate, complete, and not misleading.

4.8 Anonymity

- Wherever it is lawful and practicable, individuals have the option of not identifying themselves when entering into transactions with the TCHHS.

4.9 Sensitive personal information

- The TCHHS must take reasonable steps to de-identify sensitive personal information before disclosing it, except where the identifying information is required to provide services to the individual.

4.10 Transfer of personal information outside Australia

- TCHHS will only transfer personal information outside of Australia in compliance with the *Information Privacy Act 2009* and for authorised business purposes.

4.11 Exceptions to the Information Privacy Act 2009

- There are circumstances where the TCHHS is not required to comply with the *Information Privacy Act 2009*. For example, de-identified information or statistical data sets which are non-identifiable (i.e. would not allow or enable individuals to be identified).
- The TCHHS is also not required to comply with certain privacy principles where an individual has previously published their personal information or provided it for the purpose of publication.

4.12 Breaches of confidentiality and privacy

- The TCHHS will monitor and respond to suspected and actual breaches of privacy or confidentiality; including reporting to the Health Service Chief Executive.

5. Responsibilities

Position	Responsibility
TCHHS Executive Management Team	• Oversight of compliance with this policy. • Appoint key roles and responsibilities for privacy management, including a senior member of staff with overall accountability for privacy.
Information asset custodians, business owners, administrators and line managers	• Use privacy impact assessments for business projects or decisions that involve new or changed personal information handling practices (including implementing new technologies). • Ensure regular review of staff access to common and unit specific drives, email workgroups and business systems to ensure only authorised staff have access are occurring. • Promote privacy awareness by integrating privacy into induction to site and orientation to organisation activities for new starters (including short term staff, service providers and contractors).
Director Quality Safety and Risk Unit	• Implement risk management processes to identify, assess and manage privacy risks including personal information security risks.
Strategic Records Manager (Privacy Officer)	• Preliminary assessment of breaches, complaints and need for privacy impact assessments. • Deliver training on how to handle personal information in everyday duties. • Coordinate Privacy Awareness Week activities.

Position	Responsibility
Project Managers	Use privacy impact assessments for business projects or decisions that involve new or changed personal information handling practices (including implementing new technologies).
Designated persons A 'designated person' **current and previous employees** and officers of the TCHHS; the Director-General and Health Service Chief Executives; temporary staff; health professionals (including Visiting Medical Officers); anyone being educated or trained at a Queensland Health facility; contractors; and volunteers carrying out duties on behalf of the department or Hospital and Health Services.	Section 142 of Part 7 of the Hospital and Health Boards Act 2011 sets out the duty of confidentiality placed on a 'designated person'. This section states: (1) A designated person must not disclose, directly or indirectly, confidential information to another person unless disclosure is required or permitted under this Act. (2) For subsection (1), another person includes another designated person. (3) Subsection (1) applies even if the person who could be identified from the disclosure of confidential information is deceased.

6. Legislative and other Authority

- *Hospital and Health Boards Act 2011*
- *Information Privacy Act 2009 (Qld) (note National Privacy Principles)*
- *Commonwealth Privacy Act 1988*
- *Public Service Act 2008*
- *Privacy Act 1988*
- *Public Records Act 2002*

7. Supporting documents

7.1 Other procedures, process flows and guideline

- Privacy policy notice
- Security of personal information procedure (staff access only)

8. Consultation

- Chief Information Officer
- Director Quality Safety and Risk
- Human Resources Manager
- Health Information Manager
- Clinical Document Writer

9. Approval Governance Pathway

9.1 Policy Officer / Document author

The following Officer is the author of this policy

- Strategic Records Manager (Privacy Officer)

9.2 Document Custodian

The following Officer will have responsibility for implementation of this policy

- Director Quality Safety and Risk Unit

9.3 Endorsing Committee or Position

The following Officer/Committee will have responsibility for implementation of this policy

- Chief Information Officer

9.4 Approving Officer

The following Officer has approved this document:

- Health Service Chief Executive

Signature: _____ Date: _____

10. Effective Dates

- Approval date: 31/08/2017
- Effective from: 31/08/2017
- Next Date of review: 31/08/2018
- Superseded Policy: New

11. Version Control

Version	Date	Prepared by	Comments
0.1	15/08/2017	Strategic Records Manager (Privacy Officer)	
0.2	30/08/2017	Document custodian reviews finished version	
1.0	31/08/2017		

12. Audit Strategy

Risk	High
Audit strategy	RiskMan
Audit tool attached	To be developed
Audit frequency	6 monthly
Audit responsibility	Strategic Records Manager (Privacy Officer)
Indicators /Outcomes	Approved plans