Policy

TCHHS-ICT-POL-1248

Privacy

1. Policy statement

Torres and Cape Hospital and Health Service (TCHHS) is committed to ensuring the privacy, confidentiality, security, accuracy and integrity of personal information regarding all patients and families, employees, individuals and agents (including Visiting Medical Officers and other partners, contractors, volunteers and students) associated with receiving or providing TCHHS services.

TCHHS complies with relevant privacy legislation in managing the personal information lifecycle of collection, use, access, security and quality.

The *Human Rights Act 2019* (Qld) requires proper consideration to be given to human rights factors where TCHHS is contemplating a decision that may affect or limit a human right. The Privacy Policy supports compliance with the *Human Rights Act 2019* (Qld) by facilitating the proper handling and security of personal information and in this way contributing to protection of the human right of privacy and reputation.

2. Intent of this policy

This policy:

- Describes the types of personal information collected and stored by TCHHS
- Documents the principles under which personal information is used, shared and managed
- Explains how all patients, employees, individuals and agents (including Visiting Medical Officers and other partners, contractors, consultants and volunteers) can request access to, request correction of, or make a complaint regarding a privacy breach of, their personal information

3. Scope

Compliance with this policy is mandatory.

This policy applies to:

- All TCHHS clinical and non-clinical employees (permanent, temporary and casual) and all organisations and individuals acting as its agents (including Visiting Medical Officers and other partners, contractors, consultants, volunteers and students).
- All settings across the health continuum including community, primary, acute and residential care health services within TCHHS.
- All information (clinical and non-clinical), in all mediums including electronic or non-electronic (physical and hybrid) created, collected, managed, stored, disseminated and disposed of.

4. Principles

- TCHHS shall provide awareness training to staff, consultants, contractors, volunteers and students to promote understanding and compliance with the requirements of the relevant privacy legislation.
- TCHHS will promote the roles and responsibilities of the Health Information Manager and the Release of Information Officer in the management of Privacy, Confidentiality; and personal/sensitive information management within TCHHS.
- TCHHS will take all reasonable steps to protect information by the Health Service utilising information and data security measure. TCHHS will maintain procedures for the collection, use, storage and disclosure of information.
- TCHHS will promote the classification of private, personal and health information at a minimum classification of SENSITIVE in accordance with the QGCDG Information Security Classification Framework.
- TCHHS will undertake Privacy Impact Assessments (PIA) for new information systems as required.
- Where TCHHS is contracting with a service provider, and as part of the service arrangement there will be an exchange of personal information, TCHHS must take reasonable steps to bind the service provider to comply with the privacy principles within the IP Act as part of the contract or service agreement.
- TCHHS will monitor and review emerging principles in privacy against privacy practices within TCHHS to maintain legislative compliance.

5. National Privacy Principles

The *Information Privacy Act 2009* (IP Act) regulates the collection and handling of Personal and Confidential Information held by Queensland Government agencies.

TCHHS is required to comply with the privacy principles within the IP Act which include the nine National Privacy Principles (NPPs), which govern how TCHHS must handle all Personal Information.

5.1 NPP 1 – Collection of personal information

TCHHS collects personal information to:

- Provide healthcare services
- Manage the delivery of health care services
- Improve the safety, quality and effectiveness of health care services
- Manage employees, individuals and agents (including Visiting Medical Officers and other partners, contractors, consultants and volunteers) acting on behalf of TCHHS.

TCHHS collects information in the following ways:

- Information given by persons receiving, or representing those receiving, healthcare services. For example, a person's name, residential address, email address, telephone number and health information in order to provide health care.
- Information provided by other health agencies and clinicians regarding a person receiving healthcare services. For example, TCHHS will be provided with or may seek information about, a patient's health history and treatment in order to provide appropriate care.
- Information given by employees, individuals and agents (including Visiting Medical Officers and other partners, contractors, consultants and volunteers) acting on behalf of TCHHS. For example, an employee, individual or agent's name, address, work history or information related to their current work activities with TCHHS.
- Information provided by other persons or organisations about employees, individuals and agents (including Visiting Medical Officers and other partners, contractors, consultants and volunteers) acting on behalf of TCHHS. For example, TCHHS may be provided with or seek information about a person's work history, criminal history, or information related to their current work activities with TCHHS.

5.2 NPP 2 – Use or disclosure of personal information

TCHHS employees, individuals and agents (including Visiting Medical Officers and other partners, contractors, consultants and volunteers) acting on behalf of TCHHS are legally bound to a duty of confidentiality and will not use or disclose personal information unless:

- It is for the primary purpose for which the information was collected, and the individual would expect disclosure
- The individual has consented
- It is necessary for 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, or
- It is authorised or required by law.

TCHHS employees, individuals and agents will ensure that any such disclosure is limited to only what is necessary. On occasion, personal information may be used for training or research that will help to improve TCHHS services without explicit consent. All research involving TCHHS held personal information must undergo ethics consideration, be strictly managed for privacy and confidentiality, and be authorised by the Chief Executive before it can be conducted.

Patient confidentiality in Queensland public sector health services is strictly regulated. Part 7 of the *Hospital and Health Boards Act 2011* (Qld) (HHBA) sets out the duty of confidentiality and exceptions that permit disclosure of Confidential Information by 'designated persons', including TCHHS employees, individuals and agents acting on behalf of TCHHS.

It is an offence to disclose Confidential Information about a person unless one of the exceptions in Part 7 of the HHBA applies.

5.2.1. De-Identified Information

Where information has been de-identified so that an individual's identity is no longer apparent or reasonably ascertainable, then the information will not be subject to the IP Act or the HHBA.

Typically, this would be aggregated information or statistics used for reporting, research and planning purposes where identifying information has been removed or altered. However, as technology changes and the ability to combine different datasets increases, so does the possibility of re-identification of an individual's data. For this reason, TCHHS will continue to review its de-identified data sets as part of its information management and data custodianship responsibilities to ensure that privacy and confidentiality is not being compromised. For further information on deidentification refer to the Definitions for identifiable, de-identified, non-identifiable, re-identified and anonymised data.

5.2.2. Transfer of personal information outside of Australia

TCHHS employees, individuals and agents acting on behalf of TCHHS are legally bound **not to** transfer personal information outside of Australia, except under specific circumstances described in the IP Act.

5.3 NPP 3 – Quality of personal information

TCHHS will take reasonable steps to ensure the personal information it collects, uses or discloses is accurate, complete and up to date.

5.4 NPP 4 – Security and management of personal information

The *Public Sector Ethics Act 1994* (Qld) as articulated through the Queensland Public Service Code of Conduct obliges all TCHHS employees, individuals and agents to uphold ethical principles and values, and to comply with all relevant legislation, policies and standards.

Section 4.4 of the Code specifically requires all TCHHS employees, individuals and agents to:

- 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, and
- Not use confidential or privileged information to further personal interests.

Consequently, TCHHS employees, individuals and agents:

- **Will not** use information gained through their connection with TCHHS for any purpose other than for the discharge of their official duties.
- **Will** take reasonable steps to protect personal information from misuse, loss and unauthorised access, modification or disclosure. When personal information is no longer required, it is destroyed in a secure manner according to Queensland State Archives' approved retention and disposal schedule and relevant TCHHS policies and procedures.
- **Will** take reasonable steps to ensure information management policies, procedures and systems are designed to implicitly support privacy and confidentiality.

5.5 NPP 5 – Openness

TCHHS has a Privacy Plan which describes the types of information generally collected by TCHHS and how personal information is managed within TCHHS.

5.6 NPP 6 – Access to personal information

TCHHS patients, employees, individuals and agents may request access to their personal information. Further detail on making an access application is available on the TCHHS Release of Information webpage.

5.7 NPP 7 – Amendment of personal information

TCHHS will take reasonable steps to ensure the accuracy of personal information and will, where reasonable, amend personal information when requested to ensure it is accurate, complete and not out of date or misleading. Further detail on making an access or amendment application can be found on the TCHHS Release of Information webpage.

5.8 NPP 8 – Anonymity

Individuals may have the option of not identifying themselves when entering transactions with health agencies including TCHHS, if it is lawful and practicable to do so. For example, it may not be practicable where the identity of the person is important to the delivery of the service, such as in the prescribing of medications and allergy information.

5.9 NPP 9 – Sensitive information

Sensitive information, as defined in Section 10 – Definition of terms, is not collected unless:

- The individual has consented
- It is required by law
- It is necessary to prevent or lessen a serious threat to the individual
- The information forms part of a family medical or social history and is collected for the purpose of providing a health service.

6. Privacy breaches and privacy complaints

TCHHS takes breaches of privacy very seriously and will take prompt action to investigate and to minimise the impact of any potential breaches. The Release of Information Officer or the Health Information Manager, should be contacted in the first instance with either a potential privacy breach or for any privacy complaints.

Complaints must be dealt with within 45 business days. Where a complainant is dissatisfied then they have the right to review by the Office of the Information Commissioner.

7. Listening Devices

TCHHS employees, individuals and agents acting on behalf of TCHHS are legally bound by the *Invasion of Privacy Act 1971 (Qld)*.

The following are offences, unless permitted under the *Invasion of Privacy Act (971) Qld*:

- Use of a listening device to overhear, record, monitor or listen to private conversations.
- Communicating or publishing a private conversation overheard, recorded, monitored or listened to by a listening device.
- Publishing or communicating any record of a private conversation to which a person was a party and used a listening device to overhear, record, monitor or listen to that conversation.

Executive Officers can be found personally liable if the organisation commits an offence under Section 49A of the *Invasion of Privacy Act 1971 (Qld)*.

8. Partnering with consumers

Consumers should be referred to the Release of Information Officer when they are seeking access to or amendment of their medical records. Staff should also refer consumers to the Release of Information Officer when consumers wish to make a privacy complaint.

When collecting personal information, staff are responsible for providing information to consumers about what TCHHS will do with the information collected and who it will be shared with, in a way that is understandable and that meets their needs.

9. Responsibilities

Position	Responsibility
Executive Management Team	• Oversight of compliance with this policy. • Appoint key roles and responsibilities of privacy and confidentiality management, including an Executive member of staff with overall accountability for privacy.
Information asset custodians Project Managers	• Use Privacy Impact Assessments for business projects or decision that involve new or changed information handling practices, including implementing new technologies.
Line Managers	• Promote privacy awareness by integrating privacy and confidentiality into orientation and induction activities for new starters. • Ensure regular review of staff access to common and unit specific network drives, email workgroups and business systems to ensure only authorised staff have access.

Position	Responsibility
Director Clinical Governance Unit	• Implement and promote processes to identify, assess and manage privacy risks, including personal information security risks.
Health Information Manager Digital Services Manager	• Preliminary assessment and reporting of breaches and privacy complaints.
Release of Information Officer	• Delivery of training on how to handle Confidential, Personal and Sensitive Information.
Designated Persons (All Staff)	• Comply with this policy. • Comply with privacy and confidentiality requirements of the IP Act and HHB Act. • Comply with requirement of the *Invasion of Privacy Act 1971 (Qld)*.

10. Supporting documents

10.1 Legislation / standard/s

- Standard 1 – Clinical Governance
- *Commonwealth Privacy Act 1988*
- *Hospital and Health Boards Act 2011*
- *Human Rights Act 2019*
- *Information Privacy Act 2009*
- *Invasion of Privacy Act 1971*
- *Public Records Act 2002*
- *Public Sector Ethics Act 1994*
- *Public Service Act 2008*

10.2 Other procedures, process flows and guidelines

- Privacy and Confidentiality of Patient Information Procedure
- Privacy and Confidentiality Procedure
- Office of the Information Commissioner - Dataset publication and privacy
- Office of the Information Commissioner - Dataset publication and de-identification techniques
- De-identification and anonymisation of data guideline

10.3 Forms and templates

- DoH Privacy Impact Assessment – Assessment Tool
- DoH Privacy Impact Assessment Template

11. Related documents

- TCHHS Privacy Plan
- DoH Privacy Plan
- Privacy Policy Notice
- TCHHS RTI and IP Delegation Manual

12. Definition of terms

Term	Definition / explanation / details	Source
Availability	Information availability refers to how accessible information is for an intended user or audience at the time the information is required.	QGCDG Information Security Classification Framework.
Confidential Information	Confidential information means 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, *Hospital and Health Boards Act 2011*
Confidentiality	Confidentiality is the act of not disclosing personal information without authority, i.e., keeping personal information private or in confidence.	*Hospital and Health Boards Act 2011* Office of the Information Commissioner
Designated Person	A full definition of "Designated Person" can be found at s.139 HHB Act. It includes all current and previous employees and officers of TCHHS, including temporary staff; visiting health professionals; anyone being educated or trained at a TCHHS facility; contractors; volunteers and other partners carrying out duties on behalf of TCHHS.	Section 139, *Hospital and Health Boards Act 2011*

Term	Definition / explanation / details	Source
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.	
Integrity	Information integrity refers to how well the information reflects its underlying subject	QGCDG Information Security Classification Framework.
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. 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).	Section 12, Information Privacy Act 2009
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.	Information Privacy Act 2009
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.	Information Privacy Act 2009 Office of the Information Commissioner
Privacy Impact Assessment	A Privacy Impact Assessment (PIA) is a due diligence exercise and a strong risk management tool. PIAs assist business areas to confidently assess the privacy risks of proceeding to the implementation phase of an initiative. The PIA is designed to identify specific privacy issues and risks that must be addressed during the development of a new system to ensure compliance with Queensland Health information handling requirements	Department of Health: Privacy and Right to Information Unit – PIA Template

Term	Definition / explanation / details	Source
Private Conversation	Any words spoken by one person to another person in circumstances that indicate that those persons desire the words to be hears or listened to only by themselves; or that indicate that either of those persons desires the words to be hear or listened to only by themselves and some other person, but does not include words spoken by one person to another in circumstances in which either of those persons ought reasonably to expect the words may be overheard, recorded, monitored or listened to by some other person, bot being a person who has the consent, express or implied, of either of those persons to do so.	*Invasion of Privacy Act 1971 (Qld)*
Sensitive Information	Sensitive Information about an individual, for the NPPs, means: (a) personal information about the individual that includes any of the following: (i) the individual's racial or ethnic origin; (ii) the individual's political opinions; (iii) the individual's membership of a political association; (iv) the individual's religious beliefs or affiliations; (v) the individual's philosophical beliefs; (vi) the individual's membership of a professional or trade association; (vii) the individual's membership of a trade union; (viii) the individual's sexual preferences or practices; (ix) the individual's criminal record; or (b) information that is health information about the individual for the NPPs The use of the SENSITIVE indicates that information requires additional handling care due to its sensitivity or moderate business impact if compromised or lost. SENSITIVE information must be labelled	Schedule 5 – Dictionary, Information Privacy Act 2009 QGCDG Information Security Classification Framework.

13. Consultation

- Executive Director Finance, Information & Digital Services
- Director Clinical Governance Unit
- Human Resources Manager
- Digital Services Manager
- Release of Information Officer

14. Approval governance pathway

14.1 Document author

The following officer is the author of this policy

- Health Information Manager

14.2 Document custodian

The following officer will have responsibility for implementation of this policy

- Executive Director Finance, Information & Digital Services

14.3 Endorsing position

The following officer will have responsibility for implementation of this policy

- Executive Director Finance, Information & Digital Services

14.4 Approving officer

The following officer has approved this document

- Health Service Chief Executive

Signed: 09/09/2021

15. Effective dates

Schedule	Dates
Approval date	09/09/2021
Effective from	09/09/2021
Next date of review	09/09/2023
Superseded policy	V 1.0

16. Version control

Version	Date	Prepared by	Comments
1.0	31/08/2017		Approved by HSCE
1.1	06/12/2019	J Foster	Document checked, analysed and edited to comply with *Human Rights Act 2019.*
1.2	11/06/2021	M Jeffress	Policy reviewed and consolidated
1.3	05/08/2021	M Jeffress	Incorporation of stakeholder feedback
1.4	06/09/2021	M Jeffress	Add information relating to *Invasion of Privacy Act 1971 (Qld)* to the policy.
2.0	09/09/2021		Approved by HSCE

17. Evaluation strategy

Strategy	Evaluation
Risk	Consequence rating – Major Likelihood rating – Unlikely Overall risk rating – Medium (14)
Evaluation strategy	Document review, identifying and evaluating compliance. All requests will meet their relevant legislative timeframe and/or appropriate requested timeframe.
Frequency	Yearly
Evaluation responsibility	Release of Information Officer

18. Document communication and implementation plan

Action	Responsible position
Identify the target group • TCHHS staff	Executive Director Finance, Information & Digital Services
Provide a timeline for communication and implementation milestones • Upon publishing	Health Information Manager
Identify method of communication • TCHHS Weekly Newsletter • QHEPS Publishing	Communications and Media Officer
List education and training available to support implementation • Staff Orientation • Privacy / Confidentiality Training • Targeted training sessions, as requested	Line Managers Release of Information Officer
Identify frequency of communication • On initial publication and then on updates.	Health Information Manager

19. References

CHHHS Privacy and Confidentiality of Personal Information Policy

THHS Privacy and Confidentiality Policy

MNHHS Privacy Policy