Policy Applies to:
All members of staff; Compliance will be facilitated by Mercy Hospital staff for Credentialed Specialists; Contractors, Students and where relevant, Visitors and Patients

Related Standards:
Mercy Hospital complies with the following legislation in relation to privacy issues;

1. Health Act 1956 section 22f covers disclosure of information to the individual, their representative and or a health provider.

2. The Privacy Act 2020 controls how 'agencies' collect, use, disclose, store and give access to 'personal information'. The Act is primarily concerned with good personal information handling practices but does not apply when another law authorises or requires information be made available or requires an action. The Privacy Act also requires all organisations to have a specifically designated person as a Privacy Officer. The Privacy Act has 13 Principles;

a) Principle 1, Principle 2, Principle 3 and Principle 4 govern collection of personal information, why it may be collected, where it may be collected from, and how it is collected.
b) IPP 1, only collect a person's identifying information if it is necessary
c) IPP 4 Particular care to only collect information from children and young people in ways that are fair and reasonable under the circumstances
d) Principle 5 governs personal information storage to ensure no unauthorised use or disclosure.
e) Principle 6 the right to access information about themselves. Unless access would endanger someone's safety or involve an unwanted breach of someone else's privacy
f) Principle 7 the right to correct information about themselves.
g) Principle 8 ,9, 10 and 11 place restrictions on how people and organisations can use or disclose personal information, including ensuring information is accurate and up-to-date, that it isn't improperly disclosed, and that is only held for the period it is required for the purposes for which it may lawfully be used.
h) Principle 12 specifies criteria to be met for the disclosure of personal information outside of New Zealand
i) Principle 13 governs how "unique identifiers" - such as IRD numbers, can be used. Must take reasonable steps to protect unique identifiers from being misused.

3. The Health Information Privacy Code 2020 is a code of practice issued by the Privacy Commissioner and replaces the 13 privacy principles with 13 rules that apply to health agencies:
   Rule 1 Purpose of collection of health information
   Rule 2 Source of health information
   Rule 3 Collection of health information from individual
   Rule 4 Manner of collection of health information
   Rule 5 Storage and security of health information
   Rule 6 Access to personal health information
   Rule 7 Correction of health information
   Rule 8 Accuracy, etc., of health information to be checked before use or disclosure
   Rule 9 Retention of health information

Rule 10 Limits on use of health information
Rule 11 Limits on disclosure of health information
Rule 12 Disclosure of health information outside of New Zealand
Rule 13 Unique Identifiers

Ngā Paerewa Health and Disability Services Standards NZS8134 2021

Rationale

This policy ensures practices concerning privacy and release of information comply with the identified legislation and standards for patients and staff at Mercy Hospital.

Cultural Considerations

The enforcement of the Privacy Act depends on a complainant being able to establish some harm or loss, that concept is directly translatable to a "loss of mana".
Some information is seen as particularly culturally sensitive, such as whakapapa. In recognition of the particular cultural considerations associated with privacy and information in Māori kaupapa, Mercy has a responsibility to consider the needs and values of Māori and different cultural groups when considering privacy issues.

Definitions:

Privacy principles: rules of collection, storage, access & correction, accuracy, retention, use, disclosure and personal identifiers.

Confidentiality: like secrecy. Fundamental to trust relationship as promotes full disclosure. May disclose if authorised, in emergency or in public interest.

Security: Protection from unauthorised disclosure (or use, alteration, deletion).

Data breach: is when there is unauthorised or accidental access to or disclosure of personal information.

Data breach notification is the practice of notifying affected individuals and the Privacy Commissioner when their personal information has become available to unauthorised individuals or organisations if this breach has, or is likely, to cause serious harm Serious Harm for example

- Where there is a risk of identity theft or fraud
- Where there is a risk of physical harm
  Where there is a risk of humiliation, loss of dignity or damage to a person's reputation

Authorised Agent for Release of Information:

- a person authorised by the patient to have access to their Clinical Records
- a person who has right of access as stipulated in the Privacy Act (parents of children under 16 years)
- a health professional or agency supporting health care who may (or in some cases may not) have the permission of the patient to access their Clinical Record.

Objectives

1 To collect only the information that is necessary from:
- the person concerned, or their nominated representative.*(HIPC Rules 1, 2, 3, 4)*
- other appropriate professionals (e.g. Radiography, Laboratories, Credentialed Specialists, or in the case of staff people such as Referees)

2. To provide the individual with details of the purpose of collecting information and identify others who may have access to it *(HIPC Rules 3, 10)*

3. To ensure that all written and electronic information which is held by Mercy Hospital is:
- secure against loss, inappropriate access, use, modification or disclosure (*H&D 2.9)*
- disposed of in an appropriate and timely way *(HIPC Rules 5, 9)*

4. To ensure that sharing of information is factual, appropriate, is limited to that which is required to adequately deal with the current situation and occurs in an environment that attends to privacy requirements *(HIPC Rules 1, 3, 8-11)*.

5. To ensure that release of written information occurs:
- as required by Statutory Obligation and Legislative Compliance:
  - Copies sent to other hospitals or medical practitioners (Health Act – Section 22f)
  - Medical Practitioners acting on behalf of ACC
- or following the completion of Release Form signed by the patient / guardian / or person with power of attorney
  - A copy of the patient's signed release form must be added to the patient's file
  - A log of all Clinical Records Requests is kept electronically in the Clinical Records Office.

6. To enable the individual concerned to have access to all information held relating to them personally and provide opportunity for correction of details *(HIPC Rules 6, 7)*

7. To ascertain the information is accurate, up to date, complete, relevant, and not misleading *(HIPC Rules 7 & 8; H&D 2.9)*

8. To systematically use unique identifiers, such as NHI number for patient and payroll numbers for staff, appropriately and accurately *(HIPC Rule 13)*

9. To ensure timely and reliable processes relating to the release of clinical records *(HIPC Rules 10 & 11)*

10. To ensure robust process in place for the disclosure of information to overseas agencies (*HIPC 12*)

11. To restrict capture of images by social media to personal use only.

Implementation

Mercy Hospital has:

- A Privacy Officer to ensure the Act and Code is upheld and to facilitate privacy education to all staff throughout the organisation. Undertakes/facilitates a privacy risk assessment for hard copy initiatives as appropriate.
- A Clinical Records Administrator (or assistant) who manages access to Clinical Records along with their compilation, storage, retrieval, tracking and, when required, copying.
- The Chief Operating Officer (COO) or a senior nurse on call who manages all requests from the coroner for out of hours urgent requests.
- A Chief People Officer (CPO) and Heads of Department who ensure adequate and secure storage, correct use and appropriate disposal of all written information relating to patients and staff.
- A Chief Information Officer (CIO) who ensures adequate and secure storage, correct use and disposal of all electronic information uses a Cloud Risk assessment (tool - appendix a privacy risk assessment- appendix for all new and existing IT systems where personal data is kept.
- A Contracts manager who ensures Privacy act compliance is incorporated into all relevant contracts with external contractors.
- Monthly digest Privacy News (office of the Privacy Commission)– dissemination to Exec/clinical management team/HODs to ensure currency
- Completion of Privacy ABC for all staff at onboarding (Tautoko). Further biennial (every two years) staff education on privacy legislation and practice requirements
- Patient Admission form and website which include a Privacy Statement
- Signage/Brochures outlining 'A patients right to privacy', 'Health Information your rights'
- Patient Information booklet beside every inpatient bed
- Complaints & Incident Policy and process

Evaluation

Evaluation of this policy will occur through;

- Patient Feedback
- Patient complaints
- Incident reports
- Privacy Audit, which includes a review of Release of Information
- Informal feedback from Staff Education
- Health One audit of access
- Awanui Labs access audits

Additional References:

External:

- Privacy Act 2020
- Health Information Privacy Code 2020
- Privacy Commission E learning privacy training modules (Privacy ABC)

- Clinical images and the use of personal mobile devices- NZMA/NZPSHA (A guide for medical students and doctors)2016
- Health Information Governance Guidelines HISO 10064:2017 MOH
- DHB General disposal authority guide (GDA)
- Privacy Commission self-assessment tool to help evaluate whether or not a breach caused (or could have caused) serious harm and if therefore notifiable. https://privacy.org.nz/privacy-for-agencies/privacy-breaches/notify-us/evaluate

Internal

- Consent Policy and appendices
- ICT Governance Policy
- Delegation of Authorities Policy
- Complaints policy
- Incident Management Policy
- ICT Security Policy
- Social media Policy
- Credentialing Policy
- Transfer of Patients Policy
- Clinical Record Management Policy
- Research Policy
- Confidentiality statement- staff/students/consumers
- Admission Information
- Patient Information Booklet (at bedside)