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

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

1. EQuIP criteria 1.6.2 Consumers-patients are informed of their rights & responsibilities

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

3. 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.

4. 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

5. in particular;
   1.4.3 Consumers are treated with respect and receive services in a manner that has regard for their dignity, privacy and independence

2.5.1 Consumers are treated with respect and receive services in a manner that has regard for their dignity, privacy and independence.

6. Health (Retention of Health Information) Regulations 1996
   Minimum retention period is 10 years beginning the day after discharge.
   (1) Requirement for consumer information to be retained
   (2) Providers are allowed to transfer health information that related to another provider; the individual concerned or, if the patient has died to a representative of that individual.

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 Director of Clinical Services (DCS) or a senior nurse who manages all requests from the Coroner for out of hours urgent requests.
- A Human Resource Manager and Heads of Department who ensure adequate and secure storage, correct use and appropriate disposal of all written information relating to patients and staff.
- An ICT Manager 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.
- Fortnightly digest Privacy News (office of the Privacy Commission)– dissemination to Exec/Senior nursing staff/HODs to ensure currency
- Biennial 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
- Feedback from Staff Education
- Health One audit of access
- SCL access audits

Additional References:

External:

- Privacy Act 2020
- Health Information Privacy Code 2020
- Privacy Commission E learning privacy training modules
- 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
- Clinical Imaging 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
- Admission Information (form)
- Patient Information Booklet (at bedside)

PROCESS

The Clinical Records Administrator, Privacy Officer and ICT Manager ensure written and electronic information relating to patients at Mercy Hospital is adequately and securely stored, used and appropriately disposed of.

a. More recent patient files up to 5 years are stored onsite
b. Files older than 5 years are stored off site but can be accessed within 24 hours via an on-line request system.

Documents older than 20 years will be destroyed.

The key consideration in the release of any information is that the person requesting the information has a right to access that information.

In relation to Clinical Records in general (there are exceptions) the following have the right to access clinical records:

- The patient,
- an authorised representative,
- Or a health provider (e.g. ACC) is requesting access to a Clinical Record.
- the person is the parent of a child under 16 years

The identity of the applicant must be verified.

In relation to all other records the appropriateness is checked by the Executive Staff member, usually the Human Resources Manager or Chief Financial Officer

The Clinical Records Administrator is responsible for providing Clinical Records as they are required:
For all admissions patient's existing clinical records can be provided as part of the patient notes

For special requests for release of Clinical Records by:

Credentialed Specialists:

The request is actioned in a timely fashion with due attention given to emergency situations as opposed to requests relating to arranged appointments.
When the whole file is required:

- It is documented by the Clinical Records Administrator on the Release of Clinical Records to Credentialed Specialists form (Appendix I), which then accompanies the file and states files are to be returned within 5 working days
- Documentation is made by the Credentialed Specialist regarding any part of the file that has been photocopied and this is subsequently kept with the Clinical Record
  Release details and return date of file are documented on Released Clinical Records Log (Appendix II), held in the Clinical Records Office.
- Any photocopying of Clinical Records by the Clinical Records Administrator is documented on the Clinical Records Administrators database for released information.
- Mercy is to be notified immediately of any privacy breaches

Access requests by consumers Patients or their Representative:

Under rule 6 of the Health Information Privacy Code, health providers who hold information about a consumer in a way that is readily retrievable must provide that consumer with access to the information if requested, as long as releasing the information is not likely

- to pose a serious threat to the life, health or safety of any individual, or to public health or safety.
- create a significant likelihood of serious harassment to an individual, s49(1)(a)(ii)
- cause significant distress to a victim of an offence, s49(1)(a)(iii).The new refusal grounds each have a high threshold before they apply, but they provide organisations with the means to find a balance in releasing information when there are other important interests at stake.

Patients or their Representative are made aware of how to access information (Patient Information Booklet). The process is initiated by completing a *Request for Access to Clinical Records form* (Appendix III), which includes clarification of the information required and verification that an appropriate person is making the request.

- The patient or their representative is able to view the record on site in the presence of the Clinical Records Administrator or an appropriate member of staff. All details are recorded on the request form.
- The patient or their representative is able to have photocopies of documents. This is documented on the request form and entered on to the Clinical Records Administrators Database for released information.
- The request is dealt with within 20 working days.
- Patient or their representative are informed of their right to access the Privacy Commissioner if they have any concerns.

Rights of access for;

- Children By parents

Section 22F of the Health Act 1956 provides that health information must be disclosed, on request, to the individual's representative or any person providing health or disability services to the individual. The parent or guardian of a child under 16 years is their representative.

Where the person holding the information reasonably believes that a disclosure of health information about a child under 16 to his or her parent or guardian would be against the child's wishes or interests, the request may be refused. Requests may also be refused on the withholding grounds in sections 24 and49-53 of the Privacy Act.

Children under 16 do not have a veto over disclosure of information to their parents. Whether a health provider will accede to a child's request that health information about them not be disclosed is within their discretion. In considering the request they should take into account the relative maturity of the child and the severity of the health matter under discussion.

If you are collecting information from children and young people you will need to;

- Explain why you're collecting the information in terms they can readily understand
- Consider whether the child might feel pressure to cooperate
- Be aware that they might not have the capacity to agree to your terms and conditions and you may need to seek parental authorisation
- Be aware they may not consider the decisions/ consequences as adults do
  The consequence of a privacy breach could be potentially worse than adults depending on the circumstances.

- 16 years and older

Under the law a child is deemed competent from the age of 16 onwards (unless factors determine otherwise). At that point the parent no longer has the right to see their child's health record without their authorisation.

- By a person who is intellectually disabled or their carer

A person with an intellectual disability has the right to see their shared record. A representative of that person, being someone lawfully acting on their behalf, may also seek access to their health record under section 22F. Access should be granted to a representative unless the disclosure would be against the wishes or interests of the person concerned, having regard to the competence of the person and the consequences if access is granted or refused.

Persons inquiring after a patient's condition should be referred to the patient if appropriate or to nursing staff. Information is to be given only to those persons nominated by the patient and identified in the Patient Admission Form.

In the case of acute transfers to another facility where the patient file accompanies the patient, a label "Please return to Mercy Hospital Dunedin ASAP", is attached. A record of patient name, NHI number and the date the file was sent is documented on Clinical Records Administrators Database. A return date is entered against this on return of the file.

All staff are required to:

a. Ensure all information is appropriately collected, checked for accuracy and only shared as necessary.
b. Practice in ways that maintain privacy of both verbal and written information including implementation of privacy requirements outlined in work manuals.
c. Participate in orientation and updates related to privacy as facilitated by the Clinical Records Administrator and Privacy Officer.

Use of Computers / Social Media by Patients and Relatives (see Social Media Policy).

While Mercy Hospital is keen to support continued access to computing & electronic devices, privacy and security are of paramount importance to us.
To assist with both privacy and security Mercy Hospital has placed signage in designated areas stating:
"We request that whilst you are a patient / visitor in Mercy Hospital, you refrain from taking visual images (photos, videos or Skype) of anyone other than yourself, and / or with their permission, images of friends and family members."

Taking visual images of staff and other patients is prohibited.

Privacy Complaints and breach of Privacy Procedure

Data breaches happen in a number of ways. Some common examples include:

- lost or stolen laptops, removable storage devices, or paper records containing personal information
- computer hard disk drives being thrown away, recycled or without the contents first being erased
- databases of personal information being hacked or illegally accessed by others outside of Mercy
- employees accessing or disclosing personal information outside their authorisation
- paper documents taken from recycling or rubbish bins
- personal information being given to the wrong person by sending information to the wrong physical or email address
- releasing personal information to a person who is fraudulently pretending to be someone else.

Privacy Breach Response Plan

Four key steps on how to respond to data breaches

These are four key steps in dealing with a data breach:

1. Contain the breach and make a first assessment
2. Evaluate the risks
3. Notify Privacy Commissioner and individual/s affected if it is considered a serious breach
4. Prevent a repeat

Move quickly to investigate the suspected breach and its potential for harm. Consider the potential for harm to the individuals to whom the data relates, harm to the public's trust in Mercy and harm to reputation.

Steps 1, 2 and 3 should be undertaken either simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies. The decision on how to respond should be made on a case-by-case basis.

Steps 2-4 are to be undertaken by the Privacy Officer, Nominated Executive Team Member or the Quality Coordinator.

STEP 1: Contain and make a first assessment

Once you have discovered that a data breach has occurred, you should quickly take common sense steps to stop the damage becoming worse:

- Immediately contain the breach. For example, stop the unauthorised practice, try and get back the records, consider disabling the system that was breached, cancel or change the computer access codes and try to fix any weaknesses in the agency's physical or electronic security.
- Notify your Executive Manager and the privacy officer (DCS) who will consider whether any external parties need to be informed. The police may need to be notified if the breach appears to involve theft or other criminal activity.
- Complete an on line incident form.
- Be careful not to destroy evidence that may be needed by Mercy or the police in finding the cause of the problem or which might allow you to fix the issue.

STEP 2: Evaluate the risks Step 2 onwards will be managed by the Privacy Officer, nominated Executive Team Members or Quality Coordinator.

To determine what other steps are needed, you need to assess the risks caused by the breach. An evaluation of the type of information involved will help you determine how to respond to the breach, who should be informed (including the Office of the Privacy Commissioner) and also whether it is appropriate to tell the individuals affected. Privacy Commission have a self-assessment tool to help evaluate whether or not a breach caused (or could have caused) serious harm and if therefore notifiable. The self-evaluation tool can be found here: https://privacy.org.nz/privacy-for-agencies/privacy-breaches/notify-us/evaluate.

Here are some factors to consider:

- Find out what kind of personal information is involved. The more sensitive the information, the higher the risk of harm to the people affected. A combination of personal information is typically more sensitive than a single piece of personal information.
- Is the personal information easy to get at? If the information is not password secured or encrypted, then there is a more real risk of it being misused.
- what is the risk of harm to people whose information has been breached?
- is there a risk of identity theft or fraud?
- is there a risk of physical harm?
- is there a risk of humiliation or loss of dignity, damage to the individual's reputation or relationships, for example, when the information lost includes mental health, medical or disciplinary records?
- what is the person's ability to avoid or minimise possible harm?
- what are the legal and contractual obligations?
- What is the extent of the breach?
- Assess whether harm could result from the breach. Is the information in the hands of people whose intentions are unknown or possibly malicious?

STEP 3: Notify affected people if necessary

- Being open and transparent with individuals about how personal information is being handled is a fundamental rule of privacy. If a data breach creates a risk of harm to the individual, those affected need to be notified. Prompt notification can help them lessen the damage by taking steps to protect themselves and regain control of that information. Your notification should include:
    - Describe breach including whether you know who has their information (but you can't tell them who that is unless you think you must to prevent serious threat to health/safety)
    - Advise of steps you have or will take in response
    - Things the individual can do to mitigate any harm they may be at risk of as a result (i.e. update passwords).
    - Confirm that the OPC has been notified, and they have a right to make a complaint to the OPC about the breach
    - Provide details of a contact person within your agency
- Do not disclose any details of anyone else affected by the breach.
- Where possible it is important to ensure you are only notifying those who have been directly impacted to avoid any undue stress. However, timely notification is a requirement of the Privacy Act and in certain scenarios it may be better to notify all who could have been affected if it is not possible to isolate precisely who the breach affected or there will be significant time lags in acquiring this information.

When to notify: It is not always necessary to notify breaches. Each incident needs to be considered on a case-by-case basis. Mercy is legally required to notify the Office of the Privacy Commissioner of serious privacy breaches.

How to notify: It is always best to notify affected individuals directly – by phone, letter, and email or in person. For particularly vulnerable people, you might need to consider notifying them through or with a support person.

STEP 4: Prevent a repeat

Don't assume that there is nothing that can be fixed or done to prevent future mistakes.

In the aftermath of a breach, Mercy will review policies and practices to minimise the collection and retention of personal information. Investigate the cause of the breach.

The amount of effort should reflect the significance of the breach, and whether it happened as a result of a systemic problem or an isolated event. It could include:

- a security audit of both physical and technical security

- a review of policies and procedures
- a review of employee training practices
- a review of any contractors caught up in the breach.

Evaluate efficacy of any changes.