Policy Applies to:

All staff employed by Mercy.

Board of Directors, Credentialed Specialists, and others involved in contributing to or accessing information at Mercy Hospital will be facilitated to comply with this policy.

Related Standards:

- Privacy Act 2020
- Health Information Privacy Code 1994
- Public records Act 2005
- Employment Relations Act 2000
- General Disposal Authority for DHBs DA262
- Retention of Health Information Regulations 1996
- HPCA Act 2003

Health and Disability Sector Standard -

EQuIP Standard 2.3 Criterion 2.3.1 Records Management systems support the collection of information and meet the organisations need.

Rationale:

To ensure that Mercy Hospital's record management systems maintain the integrity, safety, controlled access and security of all records.

Cultural Considerations:

Mercy Hospital recognise the importance of collecting, confirming, classifying, recording, storing and outputting data in a culturally appropriate manner. Specific considerations include:

- HISO Ethnicity Data Protocols (10001:2017)
- HISO Iwi Statistical Standards (10068:2017)

Definitions:

Records – refers to all clinical and non-clinical records, electronic and paper based, all other consumer / patient documented information, staff records, clinical registers, and financial information.

Objectives:

- To ensure personal information gathering complies with privacy requirements (Privacy and Release of Information Policy).
- To ensure appropriate processes and mechanisms in relation to information storage, retrieval, retention and destruction.
- To enable data to be assessed, analysed and used to:
    - Enhance patient care and services
    - Inform development and evaluation of strategic goals

- To ensure integration of information and communication technology in ways that can be utilized to enable ongoing strategic development.
- To ensure that files stored off-site are covered by appropriate contractual arrangements in terms of storage and retrieval.
- To ensure appropriate tracking when information is required off-site.
- To ensure legislative compliance.

Implementation:

- Oversight of implementation will be the responsibility of the manager of the associated areas:
    - Clinical: Clinical Services Manager; Privacy Officer; Clinical Records Administrator (Clinical Records Management Policy)
    - Human Resources: Chief People Officer (Human Resources Policy) and delegates employee on boarding and exit processes
    - Information and Communication Technology (ICT): Chief Transformation Officer (ICT Governance Policy; ICT Security Policy) and delegates level of IT access relevant to role. Removal of access on leaving Mercy
    - Finance: Chief Financial Officer.
- Contracts will reflect the objectives of this policy- supported by Contract Manager
- Education as appropriate to the individual role.
- Privacy education as a minimum every 2 years
- Documents will be disposed of using the District Health Boards General Disposal Authority as a framework. See appendix 1

Evaluation:

- Where appropriate a template for a Privacy Impact Assessment report will be undertaken see appendix 1
- Analysis and Evaluation of patient feedback and complaints
- Staff education through analysis and evaluation of audits – Clinical Records Audit; Privacy audit, Release of Information Audit
- ICT auditing processes, reactive and ad hoc Systems audits, User accounts management
    - Electronic systems that are cloud based will be assessed using a Cloud risk assessment tool see appendix 1

- Annual financial audit by external auditors, any audits conducted by the Inland Revenue.
- Subject to privacy audit requirements of HealthOne

- Internal
    - Clinical Images Policy
    - Clinical Records Management Policy
    - Contracts Management Policy
    - Consent Policy
    - Document Control Policy
    - External Service Providers Policy
    - ICT Security Policy
    - ICT Governance Policy
    - Medicine Management Policy
    - Privacy and Release of Information Policy
    - Research Policy

Appendices

- Cloud risk assessment tool

Process:

All staff will manage records to ensure:

- Principles of the privacy act are maintained when managing personal information.
    - Data is appropriately checked for accuracy and updated as required
    - Unique and personal identifiers (we are required to minimise the harm of misuse) are used (see Privacy and Release of Information Policy):
        - to ensure alignment of individual pieces of information with the health record
        - to reduce the likelihood of multiple records or misplaced pieces of information.
        - easy identification of people, with the ability to differentiate between people with the same name.

- Records are stored for the appropriate timeframe as set out in legislative requirements:
- Patient Health Records: Minimum of 15 years (Retention of Health Information Regulations 1996) General Disposal Authority for DHBs DA262, (excluding paediatric records)

    - Financial Records (7 years): (Companies Act 1993; Tax Administration Act 1994; Goods and Services Act 1985; Holidays Act 2003; Employment Relations Act 2000)
    - Human Resources Records (7 years)
    - Controlled Drug Record (10 years) Misuse of Drugs Regulations 1977
- Storage of paper-based records aims to minimise the likelihood of damage by management of heat, light, humidity, vermin and moisture, with effective fire prevention practices and detection systems in place. (Salvage of Clinical Records appendix to Clinical Records Policy)
- Storage of paper-based records off-site is contracted to 'Crown', who manage retrieval of specific files as required
- Electronic records are;
- Secured from unauthorised access, alteration or deletion (ICT Security Policy).
- To facilitate business continuity, electronic records are backed up daily. Electronic backups are duplicated with both on-site, up to two weeks history, and offsite, up to 1 year history, storage.

    - Password protected
- Electronic systems that are cloud based will be assessed using a Cloud risk assessment tool see appendix 1

- Education of all staff will be included as part of privacy training.
    - Staff are not to remove any part of a patients clinical record off site
    - Staff are not to copy any part of a patients clinical record unless this is due to a request from a patient or a duly authorised authority.