INFORMATION MANAGEMENT POLICY

Reviewed: June 2018

Policy Applies to:
All staff employed by Mercy.

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

Related Standards:
- Privacy Act 1993
- Ombudsmen Act 1975
- Health Information Privacy Code 1994
- Health Act 1956
- Hospitals Act 1957
- Companies Act 1993
- Tax Administration Act 1994
- Goods and Services Tax Act 1985
- Holidays Act 2003
- Employment Relations Act 2000
- Harmful Digital Communications Act.

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.

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 information gathering complies with privacy requirement (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: Director of Clinical Services; Privacy Officer; Clinical Records Administrator (Clinical Records Management Policy)
    - Human Resources: People and Capability Manager (Human Resources Policy)
    - IT/HR employee on boarding and exit processes- level of IT access relevant to role. Removal of access on leaving Mercy
    - Information and Communication Technology (ICT): ICT Manager (ICT Governance Policy; ICT Security Policy)
    - Finance: Chief Financial Officer.
- Contracts will reflect the objectives of this Policy.
- IT education as appropriate to the role.

Evaluation:

- Analysis and Evaluation of patient feedback and complaints
- 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
- Annual financial audit by external auditors, any audits conducted by the Inland Revenue.

Associated Documents

- **External**
    - EQuIP6; 2.3
    - Privacy Act 1993
    - Privacy Code 1994
    - Retention of Health Information Regulations 1996
    - Companies Act 1993
    - Tax Administration Act 1994
    - Goods and Services Tax Act 1985
    - Holidays Act 2003
    - Employment Relations Act 2000
    - Misuse of Drugs Regulations 1977
    - HPCA Act

- **Internal**
    - Clinical Records Management Policy
    - Human Resources Policy
    - Privacy and Release of Information Policy
    - External Service Providers Policy
    - Document Control Policy
    - Medicine Management Policy
    - Information Communication Technology Policy
    - ICT Security Policy
    - Contracts Management Policy
    - Clinical Images Policy
    - Consent Policy

Process:

- All staff will manage records to ensure:
    - Privacy is maintained
    - Data is appropriately checked for accuracy and updated as required
    - Unique and personal identifiers 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.
        - enables 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: 10 years (Retention of Health Information Regulations 1996)
    - 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
- Computer-based records are:
    - Password protected
    - Backed-up daily with storage on and off site

- Education of all staff will occur through 'Orientation' training and be included as part of privacy training.