Purpose
This policy outlines how Mercy Hospital manages information in all formats to ensure privacy, security, integrity, and utility. It supports compliance with legal obligations, operational efficiency, and Mercy's strategic goal of safe, patient-centric, and digitally enabled care.

Policy Applies to:
This policy applies to all Mercy Hospital employees, board of directors, contractors, credentialed specialists, volunteers, and any other individuals who create, access, or manage information in any form.

Policy Ownership and Governance
Policy Owner: Chief Operating Officer
Contributors: IT Manager, Chief Financial Officer, Chief People Officer, Privacy Officer
Review Cycle: Biennially or as required by legislative or operational changes

Related Standards:
- Privacy Act 2020
- Health Information Privacy Code 2020
- Public records Act 2005
- Employment Relations Act 2000
- General Disposal Authority for DHBs DA262
- Retention of Health Information Regulations 1996
- HPCA Act 2003
- HISO Ethnicity Data Protocols (10001:2017)
- HISO Iwi Statistical Standards (10068:2017)
- HISO Health Information Governance Guidelines (10029:2015)
- Ngā Paerewa Health and Disability Services Standard NZS 8134:2021 – Outcome 5.1

Health and Disability Sector Standard

This policy supports compliance with the **Ngā Paerewa Health and Disability Services Standard NZS 8134:2021**, specifically:

- **Outcome 5.1: Information Management** – *Service providers manage and protect data and information to support safe and effective service delivery.*

- This includes requirements for the secure collection, storage, access, retention, and disposal of records and information systems to ensure accuracy, privacy, and traceability across all care settings.

Rationale:
To ensure that Mercy Hospital's record management systems support the secure creation, maintenance, retention, and lawful disposal of records and documents. This ensures the integrity, safety, and accessibility of information throughout its lifecycle, in accordance with privacy legislation, operational needs, and cultural considerations.

Cultural Considerations:
Mercy Hospital recognise the importance of collecting, confirming, classifying, recording, storing and outputting data in a culturally appropriate manner consistent with Māori Data Sovereignty. Specific considerations include:

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

Definitions:

- **Records**: Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. This includes clinical and non-clinical records, in electronic or paper formats, such as patient notes, consent forms, diagnostic images, staff records, correspondence, rosters, registers, and financial records.
- **Documents**: Any written, drawn, printed, or electronic item used in day-to-day operations. Documents may become records if they are saved for compliance, reference, audit, or legal purposes. Examples include draft reports, policies, meeting minutes, or templates
- **Records Management**: The coordinated activities to control the creation, receipt, maintenance, use, and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions.
- **Document Management**: The practices used to author, edit, store, retrieve, and collaborate on documents that may or may not become formal records. This includes version control, access rights, and workflow management.
- Note: Not all documents are records, but all records must be managed in line with this policy.

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
- Support IT integration for 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): IT Manager (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:

- Privacy Impact Assessments completed as needed using approved templates
- Analysis of patient feedback and complaints specifically relating to information access, privacy, and availability
- 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
- Evaluation of all new cloud systems using the ICT Cloud Risk Assessment Tool
- Annual financial audit by external auditors, any audits conducted by the Inland Revenue.
- Subject to HealthOne privacy audits
- Awanui laboratory test results are subject to internal Awanui privacy audits.

Internal

  - 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

Process:

All staff will manage records and documents 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 10 years (Retention of Health Information Regulations 1996) General Disposal Authority for DHBs DA262, (excluding paediatric records which are 202 years)
    - 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 secured from unauthorised access (ICT Security Policy), backed up daily both on- and off-site
- Electronic systems that are cloud based will be assessed using a Cloud risk assessment tool. s
- Education of all staff will be included as part of privacy training.
    - Staff are not to remove any part of a patient's clinical record off site
    - Staff are not to copy any part of a patient's clinical record unless this is due to a request from a patient or a duly authorised authority.