

MH Policy and Procedures:	Risk rating	Extreme High	High	Medium x	Low
----------------------------------	--------------------	---------------------	-------------	--------------------	------------

Enter into Risk Management Reporting System any Breakdown in Policy, Process, Issue, Incident or suggestion to improve

AIM:

To comply with the State & National Legislation in regards to patient privacy:

National: [Privacy Act 1988](#)

QLD: [Information Privacy Act 2009 \(Qld\)](#)

And the Montserrat Day Hospital Privacy Policy and Data Breach Response Plan to maintain confidentiality of patient, staff and business information.

KEY POINT OF POLICY:

NO information is to be released without approval of an Executive Member

Definitions

Personal Information: Is any information about an individual which identifies the individual or which allows his or her identity to be reasonably ascertained. In the Hospital context, examples of personal information include home address, home telephone number, date of birth, marital status, next of kin; salaries and wages of Hospital staff; all information concerning staff, their clinical performance and their personal welfare (such as medical matters, Medicare numbers, Private Health Insurance details and banking details).

Associated Policy/Procedure

- MDH Code of conduct
- MDH Student Placement procedure
- MDH Agency Staff Procedure
- MDH Confidentiality Agreement deed
- MDH Data Breach Response Plan

PROCESS:

Collection of personal information: Personal information will be collected in a way which is lawful, fair and not unreasonably intrusive to the privacy of the individual concerned. Reasonable steps will be taken to:

- Ensure that the information is up to date, accurate and complete
- Inform the person why the information is being collected and how it is intended to be used.

Personal information about an individual collected for a particular purpose is not to be used for another purpose. The exceptions are where:

- the individual consents to the information being used for the other purpose;
- the proposed use is necessary to prevent or lessen a serious threat to life, health, safety or welfare of the individual or the public generally;
- the proposed use is authorised or required for the enforcement of the law;

DOCUMENT TITLE: POLICY & PROCEDURE TEMPLATE	VERSION NUMBER: 1.2	NEXT REVIEW DUE: Feb 2021	APPROVED RELEASE DATE: Feb 2018
---	---------------------	---------------------------	---------------------------------

Security of Personal information: Personal information will be held securely, and will be protected from unauthorised access, use, modification and disclosure e.g. DOX Medical IT system is used to securely protect all patients medical records and Our Montserrat has appropriate security applied to each user.

Staff/Contractors and Doctors/Students Responsibility: Staff members are to take reasonable precautions to ensure that personal information obtained during the course of their duties is not disclosed, either deliberately or inadvertently, to persons who do not have a legitimate need to know the information.

- Paper-based records should not be left where they may be accessed by unauthorised persons. Medical record must be scanned into DOX then destroy the paper copy.

Disclosure of Personal Information: Personal information may be disclosed to third parties with the consent of the patient or staff member concerned. Such consent **cannot** be assumed, and should be given expressly and in writing.

Disclosure of personal information under statutory or other legal authority: In some cases, legislation has conferred upon certain public officer the right to demand and receive information, even though it would otherwise be regarded as confidential.

- a. *Income Tax Assessment Act 1937 (Cth)*
- b. Criminal Law Proceedings: personal information should not be disclosed, it may be if disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of public revenue.
- a. Occasionally, police officers involved in investigations of offences associated with Hospital activities

Until written confirmation is obtained, inspection of Hospital documents is not permitted; no personal information should be released. **Prior approval must be granted by the CEO.**

Contractors: The Hospital regularly enters into contracts for the receipt or supply of goods and services. In entering into a contract for the supply by a third party of goods or services, the Hospital will take reasonable steps to contractually bind the third party to comply with the Information Privacy Principles in the *Information Privacy Act 2009*.

Privacy Breaches: Breach of the MDH Privacy Policy Privacy may, depending on the circumstances, constitute a breach of the Hospital Code of Conduct. The Manager must report any breaches of this policy to the Director of Clinical Services as soon as practicable after the breach has been identified. An entry in the electronic risk management system should be make completed as soon as is possible.

- a. For minor breaches of the policy liaise with the relevant Manager on the necessary actions required to prevent a similar breach from occurring;
- b. For major breaches of the policy the Quality Safety Coordinator or delegate will instigate an investigation into the breach (as per the MDH Data Breach Response Plan). The National Data Breach Scheme (instigated Australia wide in February 2018) requires organisations to investigate all breaches and to report significant breaches to the NDBS and the Privacy Commissioner.

DOCUMENT TITLE: POLICY & PROCEDURE TEMPLATE		
VERSION NUMBER: 1.2	NEXT REVIEW DUE: Feb 2021	APPROVED RELEASE DATE: Feb 2018

- c. In order to enable a privacy breach to be properly investigated, a written complaint (is preferred) be provided to the Clinical Manager, it should identify the person whose privacy appears to have been breached. The Director of Clinical Services will have final responsibility for resolving the complaint.
- d. All staff members found to be involved in privacy breaches will be disciplined in accordance with the disciplinary policy.

Related Legislation

National: [Privacy Act 1988](#)

QLD: [Information Privacy Act 2009 \(Qld\)](#)

[Right to Information Act 2009](#)

[National Data Breach Scheme \(NDBS Feb 2018\)](#)

DOCUMENT TITLE: POLICY & PROCEDURE TEMPLATE		
VERSION NUMBER: 1.2	NEXT REVIEW DUE: Feb 2021	APPROVED RELEASE DATE: Feb 2018