Moyne Health Services	**PRIVACY, CONFIDENTIALITY AND SECURITY OF INFORMATION**		
Document Type:	Policy	**Endorsed by:**	Executive Committee
Department:	Quality & Risk	**Section:**	Quality Management

Purpose

Moyne Health Services (MHS) is committed to ensuring that the confidentiality, privacy, and security of information collected about its patients, residents, participants, clients, and staff (collectively referred to as individuals) is maintained by complying with all relevant legislation and without compromising clinical care.

MHS considers that confidentiality of individual information is essential to the provision of quality healthcare service delivery. For example, it assists individuals to freely disclose information to healthcare professionals when speaking of sensitive and personal matters, thereby facilitating appropriate diagnosis and treatment.

The unlawful disclosure of health information can bring Moyne Health Service into disrepute as well as give rise to financial penalties and claims for compensation. This policy is applicable both within and outside the workplace. Any breach of this policy may result in disciplinary action and may lead to dismissal or termination of contract/appointment. Significantly, all individuals who participate in MHS operations, or who provide services to MHS must understand that criminal penalties apply for a breach of patient confidentiality and MHS may report any such breach to a relevant authority.

Scope

All employees, credentialed personnel, volunteers, students, clinical teachers undertaking supervision of students, Board and subcommittee members and external contractors.

Definition of key words

Health Service
Incorporates all services within MHS including non-clinical areas such as People and Culture, Finance, Health Information Services, Catering, Environmental Services etc.

Privacy
The protection of the interests of the individual, and the individual's right to control how their personal information is used, and for what purposes.

Confidentiality
Confidentiality: The ethical principle or legal right that individual, other staff member or volunteer will hold secret all information relating to the individual, unless the individual gives consent permitting disclosure. Confidentiality in this context: relates to the secrecy afforded information that is, by its nature, sensitive information affecting an individual or an organisation. It can be defined as a restriction of use, disclosure and access to information that is considered to be confidential information. Business related confidential Information includes all details relating to commercial transactions or business dealings between any individual or organisation and MHS. Individual: includes but is not restricted to MHS staff, Board of Directors, Visiting Medical Officers, volunteers, members of committees and reference groups, students, observers, and all contractors undertaking work for MHS.

Security
Measures used to protect information and prevent the unauthorised use of data.

Consent
The voluntary agreement of the individual or their representative about a proposed action. It can be expressed or implied. Express consent is provided explicitly, either orally or written. Implied consent arises when consent may be reasonably inferred from the action or inaction of the individual.

Patient, Employee or Commercial Information
Includes patient/resident/client/participant or employee identifiable information stored in any medium, i.e., written, electronic or audiovisual. Financial records, memos, peer review documents, survey results, statistics, minutes of meetings, vendor contracts, policies, procedures, grievance and disciplinary process information, remuneration records etc.

Policy statement

This policy relates to all information that may identify an individual including registration details, clinical and personnel information and my health record.

Personal information may be in any form written, verbal, electronic, audio-visual, tissue samples etc.

A breach of this policy can result in:

- Disciplinary action as per the Disciplinary Policy and Procedure
- Termination of your employment or service contract
- Deregistration from professional body
- Cessation of practical placement

This policy provides guidelines, however relevant legislation should be referenced to ensure compliance with the law.

In this Document

Procedure

Patient Consent to release information for ongoing care is collected at the time of admission and confirmed with a signature on the top of the patient election form. The consent must be obtained each time the patient is admitted, and the signature must be witnessed by a staff member.

Any refusal to consent by a patient must be documented in TrakCare and an alert set up to notify staff that information cannot be released for ongoing care.

TABLE 1 outlines the appropriate responses to requests for patient information in the specified situations.

Documentation

All employees, credentialed personnel, volunteers, students and external contractors at the commencement of their employment, service agreement or practical placement are required to sign a Confidentiality Agreement held by People and Culture. Staff sign the Confidentiality Agreement on an annual basis.

Data Collection

- Only information required for the provision of health care services or human resource management purposes is to be collected.
- Information is to be collected in a manner that ensures the staff member, patient, resident, or client's right to privacy is respected at all times.
- If possible, information is to be collected directly from the employee, patient, resident, or client. In some circumstances it will be necessary to collect information from family and/or friends.
- MHS's 'Protecting Your Privacy' brochure sets out why we collect information and the laws under which we are required to collect information. This pamphlet is available at reception areas to all individuals accessing MHS for health and associated services.

Digital media for clinical purposes

- Refer to the Clinical Photography Policy that outlines guidance for the use of digital imaging in clinical settings and the process of consent regarding images taken.

Photography, filming and recording by patients / members of public.

- Individuals, their families, and friends may film or record for personal use when it is safe and appropriate to do so. There are times when taking photographs, filming or recording is not permitted if it affects the care of patients, breaches the privacy of other patients or visitors, or breaches the privacy of staff.

- Individuals, their families, and friends do not need permission to photograph, film or record themselves while in the health service as long as they do not photograph, film, or record a member of staff or any other individual or visitor. This includes capturing the voice or image of anyone nearby. This includes but is not limited to streaming or broadcasting on applications such as skype or FaceTime.
- Individuals, families, and friends must have the permission of all staff members involved in the clinical care before commencing filming. Clinical staff may direct that photography, filming or recording cease at any time.
- If individual's photographs are to be taken, permission to do so must be obtained from the individual and it must be clearly explained how/where the photograph will be used. Refer to the General Photo and Information Consent Form

Use and disclosure.

- Information of a personal nature may be disclosed only as required, authorised, or permitted under the law.
- Health information relating to an individual may be disclosed without consent for the purposes of ongoing treatment, providing that only information relevant to the current condition is disclosed in accordance with the Health Records Act 2001.
- Health information relating to an individual may be disclosed without individual consent for funding, management, planning, monitoring, improvement, or evaluation of health services provided that processes are in place to de-identify the information where possible.
- Personnel information may only be disclosed in accordance with Employee Records Policy and the Victorian Information Privacy Act.
- The Health Legislation Amendment (Information Sharing) Bill 2023 amends the Health Services Act 1988 (HS Act) to provide for the establishment of a secure electronic system to enable public hospitals and specified health services to share specified patient health information for the purpose of providing medical treatment to patients. The Bill also permits information access, use and disclosure for system establishment and maintenance, and makes consequential amendments to the Health Records Act 2001 (HR Act).

Verbal communication

- Conversations regarding individuals, staff or MHS' commercial business must not be conducted in the presence of unauthorised persons within or outside MHS.
- Communication with individuals, families and carers is an integral component of individual care. Care is aligned with the individual's expressed goals of care and healthcare needs, considers the effect of the individual's health issues and their life and wellbeing and is clinically appropriate.
- Where the individual's condition precludes them from providing consent, discussion should only be held with nominated contacts.
- Under no circumstances may a statement be made to the media, until authorised by the Chief Executive Officer or Chair of the Board of Directors.

Access to individual patient, client, resident identifiable information

Requests for individual information by non-authorised persons is to be directed to the Chief Executive Officer or General Manager Quality and Risk. If such information is required for teaching, research,

referral tools or Quality Improvement procedures, care must be taken to protect the person's anonymity and privacy. Consent must always be obtained from the individual representative, as specified in the Freedom of Information Act 1982, Health Records Act 2001, and the Information Privacy Act 2000

Requests for access to information must be in writing. If requests are made on behalf of an external organisation (e.g., Centrelink) the request must be on that organisation's letterhead. Health information may only be released in accordance with section 141 of the Health Services Act and the Health Records Act.

The following is a list of circumstances where communication (written, verbal or electronic) regarding patient, client, resident/participant identifiable information may occur. However, depending on the nature of the request, relevant legislation must be reviewed when considering the request.

- For the ongoing treatment
- When the individual (or next of kin, advocate) consents to disclosure
- When the law requires disclosure e.g., infectious diseases, Compliance with subpoena, mental health act 1986, Health services act 1988, Child information sharing scheme. Information is able to be shared without consent for the purpose of assessing or managing risk of family violence as per FAMILY VIOLENCE – IDENTIFY & RESPOND
- When disclosure is in the public interest
- For planning of health services to ensure appropriate service delivery by MHS and the Victorian Department of Health.
- For quality improvement activities to strive continually for best practice
- To conduct research in accordance with strict guidelines as determined by the MHS's ethics committee, which has been constituted in accordance with the national health & medical research council.
- For billing and payment purposes (e.g., private insurance, WorkCover, TAC, department of veteran's affairs if applicable)

Communication of information in the above circumstances must be strictly limited to information related to the function the person performs.

Access/disclosure of information required for the ongoing treatment of an individual must be limited to information relevant to the treatment of the current condition in accordance with the health services act. Access/disclosure is restricted to agencies covered by this legislation.

Care must be exercised when individual information is visible by unauthorised persons i.e., locating Acute Ward patient boards out of public viewing.

Medical records may not be taken from MHS' premises except as required for individual care at other campuses or with the prior authority of the Chief Executive Officer or General Manager of Quality and Risk.

Email

All individual identifying information being transferred outside SWARH network utilising e-mail software must be win zipped and password protected.

Refer to Information Management
Refer to Computer, Email, Web, and Social Media usage Policy

Faxing

Only urgent individual identifiable information may be sent via facsimile. Information is only to be faxed to secure clinical areas or health information services. The secure transfer of information is the responsibility of the sender.

Reproduction

Photocopying or printing of Medical Records is not to be undertaken unless:

- Approved by the General Manager Quality and Risk, or
- Approved by the Chief Executive Officer, or
- The process is in accordance with the Freedom of Information Act 1982 or
- Copies of the medical record are required to accompany a patient/resident/client being transferred to another health facility. An entry is to be made in the Progress Notes detailing:
- Document reproduced - date document(s) reproduced.
- Signature of staff member reproducing the document(s)
- Staff member must print their full name beneath the signature.

Reproduction of documents containing personal information is only permitted in the following circumstances:

- Transfer of an individual to another health care facility with an entry in the clinical notes detailing documents reproduced.
- In accordance with the Freedom of Information Act
- Compliance with relevant legislation
- When necessary for the internal management of MHS, providing copies of documents are destroyed in accordance with the destruction clause in this policy.
- De-identified documents for the purpose of research

Requests for individual information via telephone

If the identity of the caller is not recognisable, record their details and inform them that you will return the call. Establish a legitimate right to access the information, process the request and return the call.

Contacts have been recorded on TrakCare or Platinum in accordance with the Medical Treatment Planning and Decision legislation. These should be reviewed to identify that the person you are

releasing information to is listed. Document name of person you are releasing information to in TrakCare or Platinum Clinical Notes.

Staff requesting individual information e.g., Pathology results via the telephone, are to quote patient's UR no, name and date of birth.

Staff member must also identify their name, position, and clinical area from which they are calling.

Research

All research is to be conducted in accordance with strict guidelines in accordance with the Ethics committee guidelines of the Research body as applicable.

Where for scientific purposes, it is desired to publish material relating to the clinical work of MHS all published material must preserve the anonymity of patients and must be presented in a manner that does not identify an individual patient. If the identity of the individual cannot be protected, then written consent authorising release must be obtained.

Refer to Conduct of Research Policy

Disclosure of personal information to a third party

Media

Representatives of the media may only interview individuals in consultation with the individual and Chief Executive Officer.

Refer to Media and Public Comment Policy
Refer to Computer, Email, Web, and Social Media usage Policy

Police

Information should never be released without the consent of the individual, or the parent or guardian.

The only instances when information can be released to the police without the individual's consent, are:

- If there appears to be a risk of serious danger, or in a case of extreme emergency to an individual (e.g., A serious threat to their health or safety) or if there is a serious threat to public health, public safety, or public welfare.
- If a person suspects that a sexual offence has been committed against a child under the age of 16 (by another person of or over the age of 18).
- If a health professional is concerned that a holder of a firearms licence is unfit to have access to a firearm; or
- If a subpoena or warrant has been issued.
- Assessing or managing risk of family violence as per Family Violence – Information Sharing Schemes Policy.

A medical record may also be released to assist in the identification of a deceased person. Refer these requests to Chief Executive Officer and/or General Manager Quality and Risk/delegate.

General

Personal information may not be released to third parties without the consent of the individual except for ongoing treatment of an individual or disclosure in accordance with relevant legislation.

Release of individual identifiable information in all other circumstances should be via the Chief Executive Officer or General Manager Quality and Risk or respective delegates.

Sharing health and personal information for quality and safety purposes

MHS may share health and personal information (as authorised by the Health Services Act 1988) for quality and safety purposes. This would be limited to disclosing information to entities responsible for investigating failures in quality and safety and for health system quality and safety oversight, such as the Victorian Department of Health, Safer Care Victoria, the Victorian Agency for Health Information, and/or another health service entity. Any such sharing would be subject to and comply with existing data security and storage requirements set out in the Health Privacy Principles and Information Privacy Principles. The sharing and using of information is designed to address any quality and safety issues that may have affected an individual to ensure they inform continuous service improvement.

Personnel information

All requests for release of personnel information must be referred to the General Manager People and Culture or delegate.

All human resource matters including payroll details, employment contracts, disciplinary matters etc. are confidential.

Consent of the staff member is to be obtained prior to the release of information to a third party. Refer to Employee Records Policy.

Data quality

All personal information collected by Moyne Health Services must be accurate, complete, up to date and relevant to the service provided.

Data security and retention

Personal information regardless of whether electronic or hard copy storage must be protected from misuse and loss from unauthorised access, modification, or disclosure.

Mobile workstations utilised to access clinical information must not be left unattended and accessible by unauthorised persons at all times.

Health information systems must be secured by either minimising screen or logging out. All staff must log off all health information systems at the conclusion of their shift.

All information must be retained in accordance with the relevant disposal schedule for the type of information. Refer to the Document Retention Policy.

Destruction of personal information must be via a secure means.

Medical records

Under no circumstances can records, registers and other documents relating to patient/resident/participants/clients' management be inspected or information contained in them be disclosed without the authority of the Chief Executive Officer or the General Manager Quality and Risk

Requests for access to such documents may be addressed by the General Manager Quality and Risk in accordance with the Freedom of Information Act1982 or other relevant legislation. Medical Records may not be taken out of the Health Service without the prior authority of the Chief Executive Officer. Refer to Freedom Of Information Policy

The only personnel permitted to transport medical records are:

- Health professionals
- Authorised Medical records are to be transported to other authorised off-site areas in locked cases.

Destruction

All documents containing personal information or details of MHS commercial matters must be disposed of in the designated confidential bins.

Staff have a responsibility to delete information from portable electronic storage devices once reference has ceased or a hard copy placed in the medical record or on the cessation of employment with MHS.

Refer to the "General Disposal Schedule for Common Administrative Records" & the "Public Health Services Patient Information Records General Disposal Schedule" for information on:

- How long records should be kept for; and
- Suitable methods of disposal. Refer to the Disposal of Personnel Records - Patient Information Policy

Openness

Staff involved in the clinical care of the patient should be as open as practicable about the information collected and what happens to this information.

MHS' 'Protecting Your Privacy Brochure' details the process to be followed if an individual wishes to access their personal information.

Access and correction

All requests to access information held by MHS will be processed in accordance with the Freedom of Information Act, 1982. The Freedom of Information Manager will process the request and will consult with the relevant departmental head.

In accordance with the Freedom of Information Act, an individual may apply to have personal information amended.

Access to personnel records should be in accordance with the process documented in the Employee Records Policy .

Access to individual identifiable information captured electronically requires password access with levels of access approved by General Managers, Department and/or Nurse Unit Managers as applicable.

Authorisation to obtain access to TrakCare or Platinum off site is required by Managers or delegate.

Passwords for access to information captured electronically must not be shared with other staff or disclosed to unauthorised persons.

Access to personnel information captured electronically requires password access with levels of access approved by the people & culture general manager or their delegate.

Staff may only access information required for clinical management or to conduct MHS commercial functions in accordance with their role in the organisation.

Staff have a responsibility to ensure information (paper & electronic) is protected at all times from unauthorised access regardless of where the information may be held e.g., electronic devices, home office environment, vehicles, etc.

Freedom of Information requests

Individuals may request access to documents held by MHS. All requests are to be referred to the Freedom of Information Manager and processed in accordance with the Freedom of Information Act 1982 or other relevant legislation.

Refer to Freedom Of Information Policy.

Unique identifiers

Unique record numbers are utilised across MHS.

To ensure each individual is uniquely identified for the purposes of providing health services and storage of information relevant to the individual.

Transfer of personal information outside Victoria

Personal information may be transferred outside Victoria only if the recipient protects privacy under standards similar to the health privacy principles and the information privacy principles.

The sender is responsible for ensuring that the individuals' privacy will be protected from unauthorised access prior to sending the information.

Complaints

All complaints relating to an alleged interference with the privacy of an individual should be referred to the Chief Executive Officer and/or General Manager Quality and Risk.

Table 1:

TYPE OF REQUEST	STAFF INVOLVED	ACTION
MEDICAL / NURSING / ALLIED HEALTH ▪ **Must be involved in treating the patient** ▪ If the above require information for Research – refer to Research Procedure. (In Prompt)	Health Information Manager makes decision about releasing information Health Info Staff may assist with copying etc.	• Release Information
PATIENT	Health Information Staff Health Information Manager (FOI Manager)	▪ Admission & Discharge dates can be given if the patient presents in person & provides identification e.g. driver's licence. • If it is not possible for the patient to present to the Hospital proof of ID is still required. A copy of ID can be sent, and the information mailed to them. • Do not provide the details over the telephone unless urgent. Check with HIM before releasing information. ▪ If more detailed information is required refer patient to the Freedom of Information (FOI) Manager. (HIM)
POLICE	Health Information Manager (Director of Nursing in absence of HIM)	**MUST NOT BE RELEASED EXCEPT WHEN:** ▪ Patient has given consent in writing (i.e. signed & dated) ▪ Police have a subpoena or search warrant. *Note: If in the case of an urgent request that does meet the above – direct Police to HIM.*
HEALTH INSURANCE FUNDS	Health Information Staff	▪ Admission/discharge dates can be given. ▪ Diagnostic code for condition treated can be given

TYPE OF REQUEST	STAFF INVOLVED	ACTION
SOLICITORS	Health Information Manager (FOI Manager)	▪ Solicitors acting on behalf of their client may have access if they have the client's written consent. ▪ If the Solicitor requires copies of record, they are to be referred to the Health Information Manager (HIM). ▪ If the Solicitor is preparing a case against the patient, they have to obtain a court order (i.e. subpoena).
TAC **(TRAFFIC ACCIDENT COMMISSION)** **WORKCOVER** **DVA**	Health Information Staff Health Information Manager (FOI Manager)	▪ Date of Accident can be given. ▪ If medical information is required, the request is to be put in writing. Consent of the patient is required
AGED CARE DEPARTMENT **SOCIAL WELFARE AGENTS**	Health Information Manager (FOI Manager)	▪ Written consent from the patient should be obtained. ▪ There are some exceptions, always refer to the Health Information Manager.
NATIONAL DISABILITY INSURANCE AGENCY	Health Information Manager (FOI Manager)	▪ Written consent from the patient should be obtained. ▪ There are some exceptions, always refer to the Health Information Manager
DOCTOR'S ROOMS		▪ Dates of Admission/Discharge & Account Classification can be given over the telephone. ▪ A copy of a Discharge Summary can be forwarded as requested. ▪ You may be requested to read a report over the telephone – transfer this request to a HIM.
HOSPITAL / OTHER HEALTH INSTITUTIONS	Health Information Manager Outside hours – Nurse Supervisor Director of Nursing (in the absence of the HIM)	▪ In the majority of cases a copy of the Discharge Summary is sufficient. ▪ In an emergency situation information can be faxed. ▪ If in doubt, always check with HIM

TYPE OF REQUEST	STAFF INVOLVED	ACTION
PRESS / MEDIA	Refer to CEO	▪ **NO** information is to be given to the press!
STAFF		▪ NO ACCESS PERMITTED to other staff member's records! ▪ May request access to their own information – see above under "Patient"
EMPLOYERS	Health Information Manager (FOI Manager)	▪ NO ACCESS PERMITTED unless the patient has given consent in writing that the Employer can have access. ** If consent has been obtained, only information relating to the accident/condition for which the employer is financially responsible should be given* .
FRIENDS & RELATIVES	Clinical Staff	▪ DO NOT RELEASE ANY INFORMATION unless patient has given written consent. *Suggest the caller contact the patient's family if they require more information*
FUNERAL DIRECTORS	Health Information staff Health Information Manager	▪ Dates and location of Death Certificate ▪ Any additional information -Refer matter to HIM
LANDLORDS		**DO NOT RELEASE ANY INFO**
ACCOUNTS	.	▪ ONLY have access to admission/discharge dates, account classification and diagnostic codes. ▪ NOT PERMITTED to have access to medical records under any circumstances
MANAGEMENT		▪ NOT PERMITTED to have access to patient information in the medical records. *Exception would include any internal review of an FOI request, a Medico-legal case or investigation of a complaint.

References & related standards

- General disposal schedule for public health services patient information records
- Subpoena to produce documents or give evidence
- My healthrecord.gov.au
- www.health.vic.gov.au
- www.publicadvocate.vic.gov.au
- www.equalopportunitycommission.vic.gov.au
- NDIS Code Of Conduct
- NDIS Quality and Safeguards Commission

NSQHSS by Standards v2 :
1 Clinical Governance
NDIS Practice Standards and Quality Indicators :
1 Core Module - Rights and Responsibilities
2 Core Module - Provider Governance and Operational Management
Aged Care Quality and Safety Commission. Quality Standards 2019 :
1 Consumer dignity and choice
8 Organisational governance

Key aligned / linked documents.

- Protecting Your Privacy Brochure
- General Photo and Information Consent Form
- Clinical Photography Policy
- Document Retention Policy
- Freedom Of Information Policy
- Electronic Transfer of Patient Information
- Confidentiality Agreement
- Employee Records Policy
- Conduct of Research Policy
- Media and Public Comment Policy
- Document Retention Policy
- Disposal of Personnel Records - Patient Information Policy
- Password Security Policy
- Standardised Terminology Compliance

Legislation

The Health Legislation Amendment (Information Sharing) Bill 2023
Health Records Regulation 2023
National Disability Insurance Scheme (Protection and Disclosure of Information) Rules 2013
Aged Care Act 1997 (CTH)
Aged Care Quality and Safety Commission Rules 2018 (CTH)
Child Wellbeing and Safety Act 2005 (VIC)
Children, Youth and Families Act 2005 (VIC)
Family Violence Protection Act 2008 (VIC)

Guardianship and Administration Act 1986 (VIC)
Health Records Act 2001 (VIC)
Information Privacy Act 2000 (VIC)
Mental Health and Wellbeing Act 2022 (VIC)
My Health Records Act 2012 (CTH)
National Disability Insurance Scheme (Code of Conduct) Rules 2018 (CTH)
National Disability Insurance Scheme Act 2013 (CTH)
NDIS Amendment (Quality and Safeguards Commission and Other Measures) Act 2017 (CTH)
Privacy Act 1988 (CTH)
Privacy Amendment (Enhancing Privacy Protection) Act 2012 (CTH)

Risk Rating

Medium

Approval of Current Version				
	Name	**Position**	**Signature**	**Date**
Author/Reviewer:	Melissa McDonough	Quality Systems and Improvement Administrator	Melissa McDonough	03/01/2024
Consulted:	CEO/ Executive Team			8/8/2023
Approved by:	Julieanne Crow	GM Quality & Risk	Julieanne Crow	03/01/2024
Committee:	Executive Committee			8/8/2023
Changes made in this version	Privacy policy integrated with the Confidentiality and Security of Information policy. Hyperlinks inserted for legislation, NDIS standards and legislation. *Confidentiality - Release of Patient Information* policy table has been merged with this policy and has been archived.			
Education	All			
Define Risk Rating	Moderate			
FAIR	YES			