

PURPOSE

Privacy of patient's personal information must be maintained in line with relevant legislation.

PROCEDURE

This procedure includes the following sections:

- Types of patient information
- Storage
- Access
- Amendment of Information
- Medico-legal requests for information
- Subpoenas
- Data breaches
- Notifiable data breaches
- Questions and complaints

TYPES OF PATIENT INFORMATION

We may hold the following information about our patients

- Personal details including their name, date of birth, gender, marital status, address, telephone numbers, occupation and religion.
- Health Fund membership, Medicare and other identification numbers provided by the patient.
- Details of family, next of kin and emergency contact details
- Medical History
- Details of allergies, sensitivities and adverse reactions to drugs
- Current and past records of treatment provided
- GP and referring practitioners
- Other health information
- Accounting transaction details associated with our services
- Additional information provided to us by the patient
- Clinical images relating to the procedure performed for the purpose of reporting

It is the policy of the Centre for Digestive Diseases that NO photographs are allowed to be taken of patients and/or their carers without consent..

We use a patient's personal details and health information

- to provide medical treatment and care
- for administrative purposes
- to process any health fund claims

- to provide information to any practitioners providing follow up treatment or care
- for benchmarking and clinical process review to assess the safety and quality of care
- to provide data in both identified and de-identified forms to government agencies in line with legislative requirements
- to provide evidence for external third party accreditation and licensing requirements
- to refer them to another specialist for ongoing treatment

STORAGE

Our patient record are stored

- electronically in a system with secure access
- in paper based documents in secure storage facilities onsite which are destroyed by a secure document destruction company

All staff are required to sign a Confidentiality agreement on employment.

ACCESS

Patients may request access to their personal information in writing on the FM-409 Medical Records Release Form to the Administration Manager or Centre Manager. The patient is not required to provide a reason for requesting access. Proof of identity is required from the patient seeking access and this must be saved in the patient's record.

All requests are logged in the Medical Records Request Register.

The Centre Manager/Medical Director may refuse access under certain conditions. Reasons for withholding information include;

- access would pose a serious threat to the life or health of any individual
- it includes information about another person
- the request is frivolous or vexatious
- it is relevant to existing or anticipated legal proceedings and the patient would not be able to access the information in the course of those proceedings
- the law requires access to be denied

AMENDMENT OF INFORMATION

If any patient believes that personal information held by us is incorrect or inaccurate; they may request amendment of it. The Centre will consider whether or not there are grounds for amendment and this must be recorded in the record.

MEDICO-LEGAL REQUESTS FOR INFORMATION

All medico-legal requests for information are handled by the Centre Manager who may, as appropriate, involve the treating practitioner in preparation of reports for solicitors.

The request should specify the dates of treatment pertinent to the information being sought and must be an original signed version, not a copy. Requests for information must be filed in the patient's record.

All requests are logged in the Medical Records Request Register.

SUBPOENAS

The centre is under an obligation to produce only those documents covered by the description in the subpoena. A copy of the requested sections of the medical record should be provided promptly to the court. Information regarded as sensitive, correspondence and any notes that are not relevant to the case should not be produced.

All requests are logged in the Medical Records Request Register.

DATA BREACHES

A **data breach** occurs when:

- there is **unauthorised access** of personal information by someone not permitted to have access. This includes, staff, contractors and external third parties.
- there is **unauthorised disclosure** (intentional or unintentional) which makes personal information accessible or visible to others.
- there is **loss** of personal information e.g. an employee leaves personal information on public transport (e.g. hard copy documents, portable storage device)

When a data breach occurs the following action must be taken immediately it is identified:

- notify the Centre Manager and complete an FM-001 Quality Improvement Form
- act to contain the spread and distribution of the information:
 - retrieve hard/physical copies of information
 - ensure electronic copies have been deleted
 - seek written confirmation that the information has not been shared or copied
- confirm whether or not the breach is classified as notifiable which would require reporting the person whose data has been breached and/or the Australian Information Commissioner.

NOTIFIABLE DATA BREACHES

The notifiable data breaches scheme requires notification to particular individuals and the Australian Information Commissioner about "eligible data breaches". A data breach is eligible if it is likely to result in serious harm to any of the individuals to whom the information relates.

An **eligible data breach** occurs when the following three criteria are satisfied:

1. There is unauthorised access to or disclosure of personal information
2. This is likely to result in serious harm to one or more individuals
3. The centre has not been able to prevent the likely risk of harm with remedial action

If it is suspected that an eligible data breach has occurred an assessment must be conducted to determine whether it requires notification to an individual and/or the Office of the Australian Information Commissioner. Refer to <https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme>

QUESTIONS AND COMPLAINTS

Any complaints regarding management of patient's personal information should be made in writing to the Centre Manager.

If the complaint cannot be resolved by the centre it can be referred to the Office of the Australian Information Commissioner. www.oaic.gov.au

Supporting documents

Control of Records Policy
IT and Communication Technology Policies
FM-001 Quality Improvement Form
FM-409 Medical Records Release Form
FM-098 Confidentiality Agreement
My Health Record Security and Access Policy
Medical Records Request Register

References

Privacy Act 1988
Privacy Amendment (Enhancing Privacy Protection) Act 2012
Privacy Amendment (Notifiable Data Breaches) Act 2017
State Health Records Information and Privacy Act 2002