PRIVACY POLICY

POLICY

Privacy of patient's personal information must be maintained through compliance with the Australian Privacy Principles. (APP). This policy applies to the Sydney Clinic for Gastrointestinal Diseases and Newland Street Specialist Centre.

PROCEDURE

COLLECTION, USE AND DISCLOSURE:

Personal information collected will generally include:

- Patient's name, address, telephone number and Medicare number
- Date of birth and gender
- Occupation
- Next of kin details
- General Practitioner and Referring Doctor
- Marital Status
- Financial details associated with services the centre has provided
- Current drugs or treatment used by the patient;
- Previous and current medical history, including where clinically relevant a family medical history
- The name of any health service provider or medical specialist to whom the patient is referred, copies of any letters of referrals and copies of any reports back.
- Records of past and current treatment provided including intraoperative photographs

Information may be provided to a *3rd party when it is appropriate and to your benefit. * Third parties may include case review forums, insurance companies and government agencies.

APP 1 – open and transparent management of personal information – a comprehensive privacy policy is readily accessible which outlines how the organisation complies with the Act

APP 2 – anonymity and pseudonymity – individuals may choose not to identify themselves or use a pseudonym, but this is impractical and an exemption in a healthcare setting where correct identification of patients is mandatory safety and accreditation requirement

APP 3 – collection of solicited personal information - personal information must not be collected unless it is reasonably necessary for patient care

APP 4 – dealing with unsolicited personal information – this information can only be collected if it is permitted under APP3.

APP 5 – notification of the collection of personal information – patients must be notified that information is collected

APP 6 – use and disclosure of personal information – specific circumstances are defined where information can be used and released

APP 7 – direct marketing – information must not be used for direct marketing unless consent has been obtained or there is a reasonable expectation that information would be used for this

APP 8 – cross-border disclosures – if information is disclosed overseas confirmation must

be sought that it will be handled in line with the APP

APP 9 – adoption, use or disclosure of government related identifiers – cannot be adopted, used or disclosed unless an exception applies

APP 10 – quality of personal information – personal information collected must be accurate, up to date and complete

APP 11 – security of personal information – personal information must be protected from interference, misuse, loss, unauthorised access, modification and disclosure

APP 12 – access to personal information – individuals must be given access to their personal information (unless an exception applies) in a reasonable timeframe.

APP 13 – correction of personal information – reasonable steps must be taken to correct information held if identified by the organization or requested by the individual

ANONYMITY AND PSEUDONYMITY:
The APP sets out a requirement that an organisation provide individuals with an option of dealing with it using a pseudonym. This will be managed on an individual case basis, after discussion with Management & treating Specialist. It is impractical and unsafe for the organisation to deal with an individual whom have not identified themselves.

WE USE PATIENT INFORMATION:

- To provide appropriate medical/surgical treatment and care in our centre,
- To assist with any calls a patient may make to us,
- For our internal administrative requirements,
- To process private health fund claims,
- To provide information to medical practitioners and other health professionals who provide follow up treatment & ongoing care,
- For benchmarking, clinical indicator reporting and clinical review in a de-identified form,
- To provide data in both an identified and de-identified form to government agencies in compliance with numerous legislative requirements.

We will not use or disclose your personal information to any other person or organisation for any other purpose unless:

- You have consented.
- The use or disclosure is for a purpose directly related to providing you with healthcare and you would expect us to use or disclose your personal information in this way.
- We have told you that we will disclose your personal information to other organisations or persons: or
- We are permitted or required to do so under law.

STORAGE
We store patient's personal information:

- In paper based documents in secure storage within the facility,
- In electronic format with restricted access and appropriate security controls.

PRIVACY POLICY

Access to patient files shall be restricted to those personnel who need to view the contents in the course of a management or treatment activity, governing body review or compliance audit.

We keep health information for a minimum of 7 years from the date of last entry in the patient record. Records can only be removed from our premises on a court subpoena, statutory authority, search warrant, coronial summons or similar.

ACCESS TO MEDICAL RECORDS BY THE PATIENT

A patient may request access to personal information with a written signed request which includes full name, DOB, address, specific records/date range requested. The patient does not have to provide a reason for requesting access. All requests must be referred to the Director of Nursing and the doctor should be notified of the request. The centre must respond to these requests within 30 days.

The Australian Privacy Principles oblige health care providers to take reasonable steps to ensure that individuals requesting information are in fact the individuals to whom the information relates or a 'person responsible, so proof of identification is required.

Information will be checked prior to release for accuracy and completeness and to ascertain whether any information should be withheld. The treating medical practitioner is to be informed of any request prior to the information being released.

Wherever possible records are released to the patient's GP rather than to the patient directly.

Reasons for withholding information include:

- Access would pose a serious threat to the life or health of any individual,
- The information contains information about another person,
- The request is frivolous or vexatious (for example, there has been repeated requests by the same person),
- The information is relevant to existing or anticipated legal proceedings and the individual would not be able to access the information in the course of those proceedings,
- The law requires that access be denied,
- Law enforcement or national security authorities have an interest in the information requested.

Information, that is required to be withheld, should be removed from the record provided to the patient and to the patient notified that information has been withheld and the reasons.

All requests received and records of the outcome must be retained in the patient's medical record.

CORRECTION:

If an individual is able to establish that their personal information is not accurate, complete and up to date, all reasonable steps must be taken by the clinic to correct the information. If the clinic and individual disagree about the accuracy, the clinic must attach a statement to the information noting this if the individual requests it to be done.

TRANSBORDER / FOREIGN ACCESS / DISCLOSURE:

Personal information will be transferred to someone in a foreign country if:

- The individual consents to the transfer
- The transfer is necessary for the performance of a contract
- This will not breach the APPs.

USING GOVERNMENT IDENTIFIERS:
In certain circumstances we are required to collect government identifiers such as Medicare pension / Veteran Affairs numbers. We only use or disclose this information in accordance with the law..

STAFF CONFIDENTIALITY:
We require our employees and contractors to observe obligations of confidentiality in the course of their engagement and they sign confidentiality agreements.

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.

A **data breach** occurs when;

1. There is **unauthorised access** of personal information, when it is accessed by someone not permitted to have access. This includes an employee, an independent contractor or external third party.
2. There is **unauthorised disclosure**, intentional or unintentional, which makes personal information accessible or visible to others, and releases that information from its effective control in a way that is not permitted by The Privacy Act. This includes unauthorised disclosure by an employee.
3. There is **loss** (accidental or inadvertent) of personal information, in circumstances where it is likely to result in unauthorised access or disclosure e.g. an employee leaves personal information (including hard copy documents, unsecured computer equipment or portable storage devices containing personal information) on public transport.

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

1. There is unauthorised access to, disclosure of or loss of personal information
2. This is likely to result in serious harm to one or more individuals
3. The entity 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 is likely to result in serious harm, and as a result require notification to the individuals concerned and/or The Office of the Australian Information Commissioner. For details on assessing data breaches and processes for reporting refer to; https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

QUESTIONS AND COMPLAINTS
These should be referred to a Privacy Officer. Privacy Officers elected include the Practice Manager, Director of Nursing and Quality Manager.

PRIVACY POLICY

If we are unable to resolve a patient's complaint regarding information privacy it can be referred to:
The Office of the Australian Information Commissioner
PO Box 5218, Sydney, NSW 2001
www.oaic.gov.au

REFERENCES

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

RELEVANT DOCUMENTS

Personal Information Details form
Patient Personal & Privacy Information form
Complaints Management Policy
Information Technology Procedure
Cybersecurity Procedure