Hills Medical Service

Privacy & Confidentiality Policy

Purpose

To ensure patients who receive care from the Practice are comfortable in entrusting their health information to the Practice.
This policy provides information to patients as to how their personal information (which includes their health information) is collected and used within the Practice, and the circumstances in which we may disclose it to third parties.

Background

The Australian Privacy Principles (APP) provide a privacy protection framework that supports the rights and obligations of collecting, holding, using, accessing and correcting personal information. The APP consist of 13 principle-based laws and apply equally to paper-based and digital environments. The APP complement the long-standing general practice obligation to manage personal information in a regulated, open and transparent manner.
Practice procedure
The Practice will:

- provide a copy of this policy upon request
- ensure staff comply with the APP and deal appropriately with inquiries or concerns
- take such steps as are reasonable in the circumstances to implement practices, procedures, and systems to ensure compliance with the APP and deal with inquiries or complaints
- collect personal information for the primary purpose of managing a patient's healthcare and for financial claims and payments.

Staff responsibility

The Practice's staff will take reasonable steps to ensure patients understand:

- what information has been and is being collected
- why the information is being collected, and whether this is due to a legal requirement
- how the information will be used or disclosed
- why and when their consent is necessary
- the Practice's procedures for access and correction of information, and responding to complaints of information breaches, including by providing this policy.

Patient consent

The Practice will only interpret and apply a patient's consent for the primary purpose for which it was provided. The Practice staff must seek additional consent from the patient if the personal information collected may be used for any other purpose.
Collection of information
The Practice will need to collect personal information as a provision of clinical services to a patient at the practice. Collected personal information will include patients':

- names, addresses and contact details
- Medicare number (where available) (for identification and claiming purposes)
- healthcare identifiers
- medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors.

Patient's personal information may be held at the Practice in various forms:

- as paper records
- as electronic records
- as visual – x-rays, CT scans, videos and photos
- as audio recordings.

Adapted from The Royal Australian College of General Practitioners APP privacy policy: Managing patient health information August 2014.

The Practice's procedure for collecting personal information is set out below:
Practice staff collect patients' personal and demographic information via registration when patients present to the Practice for the first time. Patients are encouraged to pay attention to the collection statement attached to/within the form and information about the management of collected information and patient privacy.

During the course of providing medical services, the Practice's healthcare practitioners will consequently collect further personal information. Personal information may also be collected from the patient's guardian or responsible person (where practicable and necessary), or from any other involved healthcare specialists. The Practice holds all personal information securely, whether in electronic format, in protected information systems or in hard copy format in a secured environment.

Use and disclosure of information

Personal information will only be used for the purpose of providing medical services and for claims and payments, unless otherwise consented to. Some disclosure may occur to third parties engaged by or for the Practice for business purposes, such as accreditation or for the provision of information technology. These third parties are required to comply with this policy. The Practice will inform the patient where there is a statutory requirement to disclose certain personal information (for example, some diseases require mandatory notification).
The Practice will not disclose personal information to any third party other than in the course of providing medical services, without full disclosure to the patient or the recipient, the reason for the information transfer and full consent from the patient.

The Practice will not disclose personal information to anyone outside Australia without need and without patient consent.
Exceptions to disclose without patient consent are where the information is:

- required by law
- necessary to lessen or prevent a serious threat to a patient's life, health or safety or public health or safety, or it is impractical to obtain the patient's consent to assist in locating a missing person
- to establish, exercise or defend an equitable claim
- for the purpose of a confidential dispute resolution process.

The Practice will not use any personal information in relation to direct marketing to a patient without that patient's express consent. Patients may opt-out of direct marketing at any time by notifying the Practice in writing.
The Practice evaluates all unsolicited information it receives to decide if it should be kept, acted on or destroyed.

Access, corrections and privacy concerns

The Practice acknowledges patients may request access to their medical records. Patients are encouraged to make this request in writing, and the Practice will respond within a reasonable time. We can provide you with a form to make this request.
The Practice will take reasonable steps to correct personal information where it is satisfied they are not accurate or up to date.
From time to time, the Practice will ask patients to verify the personal information held by the Practice is correct and up to date. Patients may also request the Practice corrects or updates their information, and patients should make such requests in writing.
The Practice takes complaints and concerns about the privacy of patients' personal information seriously. Patients should express any privacy concerns in writing to our Privacy Officer. The Practice will then attempt to resolve it in accordance with its complaint resolution procedure.

Management of medical records

Confidentiality

A confidential document includes any document that links identifying information, (for instance name, date of birth or address) with personal information about that person, (for instance account details, Medicare number, and any health related information). Examples of confidential documents include pathology results, recall letters, lists of patients generated for recall, signed assignment forms, memos to doctors requesting scripts or reports etc.

Policy: All records and communications pertaining to patients are treated as confidential.

Medical records and other files containing patient information are not stored or left in areas where members of the public have unrestricted access. Records are not left open so that third parties can glance at confidential information about other patients.

Likewise, computers, faxes and printers are not available in areas where the public have unrestricted access and are protected by password access.

All staff must be aware of confidentiality requirements and recognise significant breaches of confidentiality as a "dismissible offence".

Handling of Files and Security

Each patient record is stored securely within the storage room of the surgery. The records of all "active" patients can be easily retrieved by authorised staff when required.

- The doctors, reception and management staff are all authorised to handle and manage patient confidential information.
- Reception Staff are not required, (or permitted) to read the medical record in order to be familiar with the patient's medical history.
- Cleaning and maintenance Staff are not required (or permitted) to handle confidential documents.

- External parties, for instance pharmaceutical companies and researchers are not allowed access to patient records unless the patient has given specific consent for them to do so.

Patient files are accessed by means of the patient record number. This number is accessed from Best Practice. If the computer system is down, the number can be retrieved from the computer printout of patient details. The filing room is supervised during the daytime and is locked for security at night.

No notes are placed in areas accessible to the general public.

The only time patients' records are to be taken from the surgery is for home or hospital visits. Records will be returned to the practice on the same, or the following day. A marker will be placed in the compactus indicating who has the record and when it was taken.

New patients to the practice are informed of the confidentiality of their patient record in the practice brochure.

When documents are to be disposed of, material containing personal health information must be shredded or appropriately destroyed before disposal.

Patient health information policies

Patients can access their patient file by making an appointment with the doctor to view it, they may request copies of their notes during the appointment. Patients can access copies for simple requests such as recent specialist referrals and pathology results from reception staff.
Patients are informed of the practice policy regarding our management of their personal health information by asking receptionists at the desk or doctors during a consult.

The practice will transfer patient health information to specialist or other health providers by sending a referral with a health summary and other relevant information. A patient's notes can be transferred to another practice when requested by the patient via the other practice; a patient summary with recent results and communication is sent via registered mail to the requesting practice. A patients file is not transferred via insecure methods such as facsimile, email or unregistered post; exceptions may be made for patients overseas.

The practice engages in studies and other activities that require the sending of patient health information to third parties. All patient information sent is deidentified before sending. Whenever any member of our practice team is conducting research involving our patients, we can demonstrate that the research has appropriate approval from an ethics committee.