MILLER
MEDICAL & DENTAL CENTRE

Privacy and Personal Health Information policy

Current as of: September 2023

Privacy and Security of Personal Health Information

Policy

This practice is bound by the Federal Privacy Act 1998 and National Privacy Principles, and also complies with the NSW Health Records Act 2001.

'Personal health information' a particular subset of personal information and can include any information collected to provide a health service.

This information includes medical details, family information, name, address, employment and other demographic data, past medical and social history, current health issues and future medical care, Medicare number, accounts details and any health information such as a medical or personal opinion about a person's health, disability or health status.

It includes the formal medical record whether written or electronic and information held or recorded on any other medium e.g. letter, fax, or electronically or information conveyed verbally.

Our practice has a designated person **Mr. Saravana Kumar (Director,YES IT Services)** with primary responsibility for the practice's electronic systems, computer security and adherence to protocols as outlined in our Computer Information Security policy (Refer 6.1.1). This responsibility is documented in the Contract agreement. Tasks may be delegated to others and this person works in consultation with the privacy officer.

Our Security policies and procedures regarding the confidentiality of patient health records and information are documented and our practice team are informed about these at induction and when updates or changes occur.

The practice team can describe how we correctly identify our patients using 3 patient identifiers, name, and date of birth, address or gender to ascertain we have the correct patient record before entering or actioning anything from that record.

For each patient we have an individual patient health record (paper, electronic or a combination of both, "Hybrid") containing all clinical information held by our practice relating to that patient. The Practice ensures the protection of all information contained therein. Our patient health records can be accessed by an appropriate team member when required. We also ensure information held about the patient in different records (e.g. at a residential aged care facility) is available when required.

Procedure

Doctors, allied health practitioners and all other staff and contractors associated with this Practice have a responsibility to maintain the privacy of personal health information and related financial information. The privacy of this information is every patient's right.

The maintenance of privacy requires that any information regarding individual patients, including staff members who may be patients, may not be disclosed either verbally, in writing, in electronic form, by copying either at the Practice or outside it, during or outside work hours, except for strictly authorised use within the patient care context at the Practice or as legally directed.

There are no degrees of privacy. All patient information must be considered private and confidential, even that which is seen or heard and therefore is not to be disclosed to family, friends, staff or others without the patient's approval. Sometimes details about a person's medical history or other contextual information such as details of an appointment can identify them, even if no name is attached to that information. This is still considered health information and as such it must be protected under the Privacy Act 1998.

Any information given to unauthorised personnel will result in disciplinary action and possible dismissal. Each staff member is bound by his/her privacy clause contained with the employment agreement which is signed upon commencement of employment at this Practice. (Refer Section 2).

Personal health information should be kept where staff supervision is easily provided and kept out of view and access by the public e.g. not left exposed on the reception desk, in waiting room or other public areas; or left unattended in consulting or treatment rooms.

Practice computers and servers comply with the RACGP computer security checklist and we have a sound back up system and a contingency plan to protect the practice from loss of data. (Refer 6.1.1 Computer information security)

Care should be taken that the general public cannot see or access computer screens that display information about other individuals. To minimise this risk automated screen savers should be engaged.

Members of the practice team have different levels of access to patient health information. (Refer Section 6 Compute Information security) To protect the security of health information, GPs and other practice staff do not give their computer passwords to others in the team.

Reception and other Practice staff should be aware that conversations in the main reception area can often be overheard in the waiting room and as such staff should avoid discussing confidential and sensitive patient information in this area.

Whenever sensitive documentation is discarded the practice uses an appropriate method of destruction (shredding or computer drive, memory sticks etc are reformatted)

Correspondence

Electronic information is transmitted over the public network in an encrypted format using secure messaging software. Where medical information is sent by post the use of secure postage or a courier service is determined on a case-by-case basis.

Incoming patient correspondence and diagnostic results are opened by a designated staff member.

Items for collection or postage are left in a secure area not in view of the public.

Facsimile

Facsimile, printers and other electronic communication devices in the practice are located in areas that are only accessible to the general practitioners and other authorised staff. Faxing is point to point and will therefore usually only be transmitted to one location.

All faxes containing confidential information are sent to fax numbers after ensuring the recipient is the designated receiver.

Confidential information sent by fax has Date, Patient Name, Description and Destination recorded in a log book.

Write, “Confidential” on the fax coversheet

Check the number dialed before pressing ‘SEND’

Keep the transmission report produced by the fax as evidence that the fax was sent. Also confirm the correct fax number on the report.

Faxes received are managed according to incoming correspondence protocols

The practice uses a fax disclaimer notice on outgoing faxes that affiliates with the practice.

“This facsimile transmission contains information which is confidential. This information is intended for the named recipient only. If you are not the intended recipient, please be advised that any disclosure, copying, distribution, or use of the contents of this information is strictly prohibited, and that any misdirected or improperly received information must be returned to the Practice immediately. If you have received this facsimile in error, please telephone 02 9633 7033.”

Emails

Emails are sent via various nodes and are at risk of being intercepted. Patient information may only be sent via email if it is securely encrypted according to industry and best practice standards.

Patient Consultations

Patient privacy and security of information is maximised during consultations by closing consulting room doors. All Examination couches, including those in the treatment room, have curtains or privacy screens.

When, consulting, treatment room or administration office doors are closed prior to entering staff should either knock and wait for a response or alternatively contact the relevant person by internal phone or email.

Where locks are present on individual rooms these should not be engaged except when the room is not in use

It is the doctor's/health care professional's responsibility to ensure that prescription paper, sample medications, medical records and related personal patient information is kept secure, if they leave the room during a consultation or whenever they are not in attendance in their consulting/treatment room.

Computerised Records

Our practice is considered paperless and has systems in place to protect the privacy, security, quality and integrity of the personal health information held electronically. Appropriate staff members are trained in computer security policies and procedures.