Policy and Procedure:

Security and Privacy of Records

Policy

The maintenance of privacy requires that any information regarding individual patients, including staff members who may be patients, must not be disclosed in any form (verbally, in writing, electronic forms inside/outside our practice) except for strictly authorised use within the patient care context at our practice or as legally directed.

Health records must be kept where constant staff supervision is easily provided. Personal health information must be kept out of view and must not be accessible by the public.

All patient health information must be considered private and confidential, and therefore must not be disclosed to family, friends, staff or others without the patient's consent. This information includes medical details, family information, address, employment and other demographic and accounts data obtained via reception.

Patients of our practice have the right to access their personal health information under privacy information. Our practice informs patients that they are able to access their health information. This is done via the practice information sheet, notice in the waiting area and on the practice website (if applicable).

On request for access to personal health information, our practice documents each request and endeavours to assist patients in granting access where possible and according to the privacy legislation. Exemptions to access must be noted and each patient or legally nominated representative must have their identification checked prior to access being granted.

Any information given to unauthorised personnel will result in disciplinary action, possible dismissal and other legal consequences. Each staff member must sign a confidentiality agreement on commencement of employment.

In addition to Federal legislation, our practice also complies with State or Territory legislation. Care must be taken that individuals cannot see computer screens showing information about other individuals. Screensavers or other methods of protecting information must be engaged.

Our practice is multi-disciplinary. This means we have a range of health care providers, including:

- General practitioners
- Specialists
- Nurse practitioners
- Nurses
- Allied health providers and non-clinical staff.

To ensure effective management of each patient’s health, each of the providers require access to relevant information. This information is primarily stored on the practice management software.

Access to computerised patient information is be strictly controlled with personal logins and passwords. Staff must not disclose passwords to unauthorised persons. Screens need to be left cleared when information is not being used. Terminals must also be logged off when the computer is left unattended for a significant period of time. Items for the pathology couriers or other pick ups must not be left in public view.

Our practice advises the patients of our approach on the patient registration form and in practice information.

The following words are used on the patient registration form:

Consent for use of information.

I confirm that the information I have given (on this form) is correct. I consent to sharing of all relevant information between the general practitioners, specialists, nurse practitioners, nurses, allied health providers and non-clinical staff for the purpose of managing my health. I understand this information will be used to fulfil their duties in the course of planning and managing my health care.

When not in attendance, staff must ensure that prescription pads, prescription computer generated paper, letterhead, scripts, medications, health records and related patient information are out of view. They must also be stored in areas only accessible to authorised persons.

Facsimile, printers and other electronic communication devices must only be accessible to authorised staff.

Procedure

In our practice

- Computer screens are positioned so that individuals cannot see information about other individuals
- Access to computerised patient information is strictly controlled with passwords and personal logins
- Automatic screen savers
- Computer terminals are logged off when the computer is left unattended for a significant period of time.

In our practice, prescription pads, prescription computer generated paper, letterhead, scripts, medications, health records and related patient information are stored in locked store cupboard in the staff rooms.

In our practice, the facsimile, printers and other electronic communication devices are located within consult rooms and behind reception desk.

In our practice, items for pathology couriers or other pickups are left in a secure location.

Patient Access to Records

Our practice follows this procedure on request for access to personal health information in accordance with privacy legislation:

1. Document the patient's request and forward a request to the patient's GP to check for exemptions
2. Check the patient's or legally nominated representative's identification prior to access being granted.
3. Provide personal health information within reasonable period of time as outlined in the Privacy legislation.

Helpful Resource

Office of the Australian Information Commissioner

AMA Ethical Guidelines for Doctors on Disclosing Medical Records to Third Parties 2010. Revised 2015