Privacy and accessibility of patient health information

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. (Criterion 4.2.2)

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. 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 and further information is provided in Human resource management.

In addition to Federal legislation, our practice also complies with State or Territory legislation.

Care should be taken that individuals cannot see computer screens showing information about other individuals. Screensavers or other methods of protecting information must be engaged.

Access to computerised patient information must be strictly controlled with personal logins/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.

Practice procedure

In this practice, to ensure the maintenance of privacy, health records are stored on the computer, behind the reception desk and in the storeroom (with security keypad lock) and locked cupboards.

In this 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 and computer terminals are logged off when the computer is left unattended for a significant period of time.

In this practice, items for pathology couriers or other pickups are left in the office behind the reception

Request for personal health information

Practice policy

Patients of this practice have the right to access their personal health information under the Privacy Amendment (Private Sector) Act 2000.

This 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.

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

Practice procedure

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

- Patients must make their request in writing. We document the patient's request and forward a request to the patient's GP to check for exemptions
- check the patient's or legally nominated representative's identification prior to access being granted. Photo ID should be sighted.
- Provide the information within 30 days of receiving a written request for health record information