Heidelberg Family Medical Centre

6 Tobruk Avenue, Heidelberg West, Victoria 3081
P: 03 9088 3114 F: 03 9459 5008
E: info@heidelbergfamilymedicalcentre.com.au
www.heidelbergfamilymedicalcentre.com.au

PRIVACY POLICY

Policy
National Privacy Principle 5 requires our practice to have a document that clearly sets out its policies on handling personal information, including health information.

Our Privacy statement informs patients about how their health information will be used including sending to other organizations to which the practice usually discloses patient health information and any law that requires the particular information to be collected. A signed privacy copy of their consent is scanned onto the individual patients' notes.

Procedure

We inform our patients about our practice's policies regarding the collection and management of their personal health information via:

- A sign at reception
- Our patient information sheet
- New patient forms- "Consent for the collection and use of information"
- Verbally if necessary

The privacy policy sign outlines

- What information is collected
- Why information is collected
- How the practice maintains the security of information held at the practice
- The range of people within the practice team (e.g. GPs, general practice nurses, students and allied health professionals), who may have access to patient health records and the scope of that access
- The procedures for patients to gain access to their own health information on request.
- The way the practice gains patient consent before disclosing their personal health information to third parties
- The process of providing health information to another medical practice should patients request that
- The use of patient health information for quality assurance, and professional development
- The procedure for informing new patients about privacy arrangements
- The way the practice addresses complaints about privacy related matters
- The practice's policy for retaining patient health records.

A collection statement sets out the following information:

- The identity of the practice
- The fact that patients can access their own health information
- The purpose for which the information is collected
- Other organizations to which the practice usually discloses patient health information

- Any law that requires the particular information to be collected (e.g. notifiable disease)
- The main consequence for the individual patient, if important health information is not provided.

Patient consent for the collection and use of health information is obtained on the first visit.

Once signed this form is scanned into the patient's record.
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 this 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, staff or others without the patient's approval. This is considered health information and as such it must be protected under the Privacy Act.

Any information given to unauthorised personnel will result in disciplinary action. 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 to Human Resource Management)

Personal health information is 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 or left unattended in consulting or treatment rooms.

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

Care is taken that the general public cannot see or access computer screens that display information about other individuals. To minimize this risk automated screen savers should be engaged. Privacy screens are filled to reception 2 computer screen to block the view of patients when making appointments.

Members of the practice team have different levels of access to patient health information. (Refer Section Computer 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 are 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. To help minimize this potential risk - music is played continuously in the waiting room to block out sound in the administration area.
Whenever sensitive documentation is discarded the practice uses an appropriate method of destruction – confidential cross-shredding.

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 registered postage hand delivered to Post Office for stamping, or a courier service, is determined on a case by case basis.
Copies of receipts are entered into patient electronic file.

Items for collection of 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 authorised staff.

All faxes containing confidential information are sent to fax numbers after ensuring the recipient is the designated receiver.
"Confidential" is written on the fact coversheet

Check the number dialled before pressing 'SEND'

Faxes received are managed according to incoming correspondence protocols.

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

Emails

Emails are sent 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. At this stage this practice does not send confidential health info via email.

Patient Consultations:

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

When consulting, treatment room or consulting room doors are closed - prior to entering, staff should either knock and wait for a response or alternatively contact the relevant person by internal phone, if important enough to interrupt a consultation.

It is the doctor's/nurse's responsibility to ensure that prescription paper, medical records and related personal patient information is kept secure and private, if they need to leave the room during a consultation or when they leave their consulting/treatment room.

Medical Records:

The physical medical records and related information created and maintained for the continuing management of each patient are the property of this Practice. This information is deemed a personal health record and while the patient does not have ownership of the record, he/she has the right to access under the provisions of the Commonwealth Privacy and State Health Records Acts. Requests for access to the medical record will be acted upon only if received in written format.

Both active and inactive patient health records are kept and stored securely. Records are never to be left in public or unauthorised areas of the Practice. If a doctor has borrowed a record, it is to be kept inside the consulting room in a file cabinet or returned to scanned or shred in the reception area, on the same day.

Computerised Records

Our practice 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.

Computer Information Security Policy:

Our practice has systems in place to protect the privacy, security, quality and integrity of the data held electronically. Our security policies and procedures are updated when changes occur.

The Office Manager has designated responsibility for overseeing the maintenance of our computer security and our electronic systems.

All clinical staff have access to a computer to document clinical care. For medicolegal reasons, and to provide evidence of items billed, staff, nurses and doctors always log in under their own passwords to document care activities they have undertaken.

Our practice ensures that our practice computers and servers comply with the RACGP computer security checklist and that:

- Computers are only accessible via individual password access to those in the practice team who have appropriate levels of authorization
- Computers have screen savers or other automated privacy protection devices are enabled to prevent unauthorised access to computers
- Servers are backed up and checked daily, consistent with a documented business continuity plan
- Back up information is stored in a secure off-site environment
- Computers are protected by antivirus software that is installed and updated regularly
- Computers connected to the internet are protected by appropriate hardware/software firewalls
- We have a business continuity plan that has been developed, tested and documented

Electronic data transmission of patient health information from our practice is in a secure format.

Our practice has the following information to support the computer security policy:

- Current asset register documenting hardware and software including software license keys
- Maintenance, backup including test restoration, faults, virus scans
- Folder with warranties, invoices/receipts, maintenance agreements

This Practice reserves the right to check individual's Computer System history as a precaution to fraud, workplace harassment or breaches of confidence by employees. Inappropriate use of the Practice Computer Systems, breaches of Practice Computer Security will be fully investigated and may be grounds for dismissal.

This practice has a sound backup system and a contingency plan to protect practice information in the event of an adverse incident, such as a system crash or power failure. This plan encompasses all critical areas of the practice's operations such as making appointments, billing patients and collecting patient health information. This plan is tested on a regular basis to ensure backup protocols work properly so that the practice can continue to operate in the event of a computer failure of power outage.

Procedure:

The practice computer security manual and protocols is a separate folder and based on the RACGP Computer Security Guidance. We have the following items available to enable the practice to operate in the event of a power failure - located in reception:

- Torches
- Paper prescription pads/sick certificates etc
- Appointments schedule printout and manual book
- Letterhead
- Consultation notes
- Manual credit card/payment/Medicare processing equipment
- Emergency numbers