Privacy of personal health information

Policy

As an Australian-based organisation, any data and information collected is held, used and disclosedin accordance with the *Privacy Act 1988*.

'Personal health information' is a particular subset of personal information and can include any
information collected about a person in order to provide a health service.

The information we collect about a patient can include 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 suchas a medical or personal opinion about a person's health, disability or health status.

Personal health information also includes the formal health record (written or electronic) andinformation held or recorded on any other medium (e.g. letter, facsimile, electronic, verbal).

Our practice has appointed a designated person with primary responsibility for the practice's electronic systems, computer security and adherence to protocols in accordance with **Section 6.2 -Computer information security**. This responsibility is documented in their position description.
Specific tasks may be delegated to others and this person works in consultation with the privacyofficer.

Our security policies and procedures regarding the confidentiality of patient health records and other personal information are documented and our practice team are informed about these atinduction and when updates or changes occur.

The practice team can describe how we correctly identify our patients using three (3) patient identifiers in accordance with **Section 7.6 - Patient identification** to ascertain we have selected thecorrect patient record before entering or actioning anything from that record.

For each patient we have an individual patient health record containing all clinical information held by our practice relating to that patient. Our practice ensures the protection of all information contained within these files. Our patient health records are accessed only by an appropriate team member as required, and we ensure information held about the patient in different records (e.g. at aresidential aged care facility) is available when required.

Procedure

Our practice has appointed the Practice Management with designated responsibility for ensuring theprivacy and security of personal health information held within our practice. This includes managing the practice's electronic systems, computer security and adherence to protocols as outlined and in accordance with **Section 6.2 - Computer information security**.

Our general practitioners, clinical and allied health team members and all other staff and contractors associated with this practice have aresponsibility 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 practice team members who may be patients) may not be disclosed either verbally, in writing or bycopying it either at the practice or outside it, during or outside normal opening 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 must not to be disclosed to family, friends, members of the practice team not involved in that patient's care, or any other people without the patient's approval.

Details about a person's medical history or other contextual information such as details of an appointment can sometimes still identify them, even if no name is attached to that information. Thisis still considered personal information and as such it must be protected in accordance with the *Privacy Act 1988*.

Any information given to unauthorised persons will result in disciplinary action and possible dismissal. Each member of our practice team is bound by a confidentiality agreement, which issigned upon commencement of working at our practice (refer to **Section 2.5 – Privacy and confidentiality obligations**).

The management of all practice computers and servers comply with the RACGP's *Computer andinformation security standards (CISS)* (2nd edition), and we have a sound backup system and a contingency plan to protect the practice from loss of data (refer to **Section 6.2 - Computer information security**).

Personal health information is kept where only those with authorisation can access it, and is kept out of view of and unable to be accessed by the public (i.e. not left exposed on the reception desk, inthe waiting room or other public areas; or left unattended in consulting or treatment rooms). To minimise this risk, automated screensavers are activated on all computer screens.

Members of the practice team have different levels of access to patient personal health informationas appropriate to their roles and, to maintain security all computer hardware and software passwords are kept confidential and are not disclosed to others (refer to **Section 6.2 - Computer information security**).

Any team members positioned in the practice common areas (e.g. reception and waiting areas) are made aware that conversations in these areas can often be overheard by patients and visitors and, therefore, they are to avoid discussing confidential and sensitive patient information in these areas.

Whenever sensitive documentation is to be discarded, our practice uses an appropriate method ofdestruction *shredding or security bin, reformatting computer drive, memory sticks etc.*

Correspondence
There are risks associated with electronic communication in that the information could be intercepted or read by someone other than the intended recipient. Email communications with other healthcare providers is undertaken securely through the use of encryption. Email communication with patients is discouraged; however, where initiated by the patient, the risks arecommunicated and patient consent is obtained.

Where patient information is sent by post, the use of secure postage or a courier service isdetermined on a case by case basis.

Incoming patient correspondence and diagnostic results are opened and viewed only by adesignated practice team 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 team members. Faxing is point to point and will, therefore, usually only be transmitted to one location.

All facsimiles containing confidential information are sent only after ensuring the facsimile numberdialled is the designated receiver before pressing ‘Send’.

Details of confidential information sent by facsimile are recorded in a designated logbook which incorporates the date of transmission, patient name, description of the contents and the designatedreceiver (name and facsimile number).

A copy of the transmission report produced by the facsimile is kept as evidence that the facsimilewas successfully transmitted, and as evidence the information was sent to the correct facsimile number.

Facsimiles received are managed according to incoming correspondence protocols.

The words ‘Confidential’ are to be recorded on the header of the facsimile coversheet and a facsimile disclaimer notice at the bottom of all outgoing facsimiles affiliated with the practice.

The following are the details of the practice’s facsimile disclaimer notice.

Breach of confidentiality & accidental breach of confidentiality

Patient consultations
Patient privacy and security of information is maximised during consultations by closing the consulting room doors. When the consulting, treatment room or administration office doors are closed, practice team members must ensure they knock and wait for a response prior to entering.

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

It is the general practitioner/healthcare team member's responsibility to ensure that prescriptionpaper, patient health records and related personal information is kept secure if they leave their room during a consultation or treatment, or whenever they are not in attendance in the consulting/treatment room.

Patient health records
The physical health 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 personalhealth record and while the patient does not have ownership of the record, he/she has the right to access under the provisions of the *Privacy Act 1988*. Requests for access to a patient's health record will be acted upon only if the request is received in written format.

Both active and inactive patient health records are kept and stored

securely.A patient health record stored electronic in Medical Software

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

Members of the practice team have different levels of access to personal patient health informationas appropriate to their roles and to maintain security all computer hardware and software passwords are kept confidential and are not disclosed to others (refer to **Section 6.2 - Computer information security**).

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 computersecurity policies and procedures.

Members of the practice team have different levels of access to patient personal health informationas appropriate to their roles and to maintain security all computer hardware and software passwords are kept confidential and are not disclosed to others (refer to **Section 6.2 - Computer information security**).

Our general practitioners and other healthcare team members, including locums, are made aware ofand ensure that a record is to be made for every consultation are computerised health record system, indicating where the clinical notes for the consultation are recorded.

To enhance privacy, security and confidentiality, patient health records are never placed on top of the reception counter and when a general practitioner or other healthcare professional (e.g. nurse,allied health) requests a record or are to see a patient, the records are scanned in patient file.