Your Privacy Your Choice

The doctors and staff of this practice are committed to giving you our valued client quality care and service.

We protect your privacy and treat all patient information including health and financial details as private and confidential. We have developed and documented a privacy policy according to current privacy laws*. Doctors and staff of this practice abide by this privacy policy and understand that a policy breach is grounds for dismissal.

Our Privacy policy states

- What type of personal information we collect
- Purpose of collecting your personal information
- How we collect and store information
- How we use, protect and disclose information
- That we need your consent to collect your information
- That you have a right to access your information
- How to access your personal information
- That you may discuss any concerns you have about how we handle your information
- How you can make a complaint about possible privacy breach

If you would like more information about privacy, or how to access your health record please ask your doctor or see reception. * www.sa.gov.au Privacy Act 1988. Implemented January 2017

Privacy & Medical records

6.1	**Privacy & Security of Personal Health Information** ☑ 4.2.1&3.1.4	
	6.1.1	Computer Information Security ☑ 4.2.1 & 4.2.2
	6.1.2	Practice Privacy policy ☑ 4.2.1
6.2	3rd Part Requests for Access to Ppersonal Health Information Under Privacy legislation ☑ 4.2.1	
6.3	Patients Request for Access to Personal Health Information Under Privacy Legislation ☑ 4.2.1	
	6.3.1	Privacy Officer ☑ 4.2.1
	6.3.2	Privacy Audit
6.4	Medical records Administration ☑ 3.1.4	
	6.4.1	Creating a new medical record
	6.4.2	Retrieving a medical record for a current Patient ☑ 4.2.1
	6.4.3	Filing Reports (Pathology Ultrasound Consultants etc)
	6.4.4	Errors in medical records
	6.4.5	Allergies & Alerts ☑ 1.7.2
	6.4.6	Back Up of Electronic Medical records
	6.4.7	Retention of Records and Archiving ☑ 4.2.2 & 4.2.1 & 1.7.1
	6.4.8	Transfer of Medical Records ☑ 4.2.1 & 4.2.2
	☑ Indicates applicable 4th Edition RACGP Standards ☑	

6.1 Privacy and Security of Personal Health Information Policy

This practice is bound by the Federal Privacy Act (1988) and National Privacy Principles.

'Personal health information' is 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 Dr Rachel Earl with primary responsibility for the practice's electronic systems, computer security and adherence to protocols as outlined in our Computer Information Security Policy (Refer Section 6). This responsibility is documented in the Position Description. 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 is 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 Electronic patient health record 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.

For more information visit the federal privacy commissioners website at www.privacy.gov.au or go to the state health service commissioners at www.dhs.gov.au/privacy.

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 patience 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 the information. This is still 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 and possible dismissal. Each staff member is bound by his or her privacy clause contained within 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 you and access by a public e.g. 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 have a sound backup system and a contingency plan to protect the practice from loss of data. (Refer section six computer information security.) Care should be taken that the general public cannot see or access computer screens that display information about of individuals. To minimise this risk automatic screensavers should be engaged.

Members of this practice team have different levels of access to patient health information. (Refer section 6 computer information security.)

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, a locked confidential waste bin is stored on site.

Whenever sensitive documentation is discarded the practice uses an appropriate method of destruction – a locked Confidential waste bin is stored on site.

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 registered postage or a career services determined on a case by case basis. Incoming patient correspondence and diagnostic results are opened by does it needed staff members. Items for collection or postage are left in a security area not in view of the public.

Facsimile

Fax printers and other electronic communication devices in the practice are located in areas that are only axis of all to the 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 designated receiver. Keep the transmission report produced by the facts as evidence that the fax was sent. Also confirm the correct fax number on the report. Faxes received to manage according to incoming correspondence protocols (Refer section 6.) The practice uses a fax disclaimer notice on outgoing faxes that affiliates with the practice: (If you are not the intended recipient of this fax please return the fax number above and shred.)

Emails

Emails are sent via various nodes and are at risk of being intercepted. Patient information may only be sent via email if it have securely encrypt it according to industry and best practice standards. Patient consent is sought for any email correspondence.

Patient Consultations

Patient privacy and security of information is maximise during consultations by closing consulting room doors. When consulting treatment room or Administration office stores are closed staff should either knock, and wait for response, all turned simply 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 doctors/healthcare professionals 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 whether they are not in attendance in their consulting/treatment room.

Medical records

The physical medical records and related information created and maintained for the continuing management of each patient property of this practice. This information is to 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 and written format. (Refer section 6 patient request for access to personal health information under the privacy legislation.)

Our patient health records can be accessed by an appropriate team member when required. All staff member have personal passwords, which are known only to them. Both active and inactive patient health records are kept and stored securely. (Section 6 retention of records and archiving)

Computerised records

This 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.

State & Territory privacy legislation resources for health professionals www.privacy.gov.au/ Mental health services in the privacy sector – meeting privacy obligations. http://pmha.com.au/ Portals/4/public documents/privacy kit for mental health service providers/privacy%20kit%20for%. Australian charter of healthcare rights include seven charter rights – Access, safety, respect, communication, participation, privacy, and comment, www.health.gov.au/Internet/safety/publishing.NSF/content/priority program-01

6.1.1 Computer information security

Policy

Practice has systems in place to protect the privacy, security, quality and integrity of the data held electronically. Doctors and staff are trained in computer use and our security policies and procedures and updated when changes occur. Dr Rachel EARL has designated responsibility for overseeing the maintenance of our computer security and our electronic systems. All clinical staff has access to a computer, to document clinical care. For medico legal reasons, and to provide evidence of items built in the event of a medical audit. Staff especially nurses always looking under their own passwords to document care activities they have undertaken.

Our practice insures that our practice computers and service comply with the standard required of a medical practice security checklist:

– Computers are only accessible via individual password access to those in the practice team of appropriate levels of authorisation.

– Computers have screensavers or other automated privacy protection devices are unable to prevent unauthorised access to computers.

– Servers are backed up and checked at frequent intervals, consistently documented business continuity plan.

– Backup information is stored in a secure offsite environment.

– Computers are protected by antivirus software that is installed and updated regularly.

– Computer is connected to the Internet are protected by appropriate hardware/software firewalls.

– We have a business continuity plan has been developed, tested and documented.

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

Our practice is the following information to support the computer security policy

– Current asset register documenting hardware and software including software license keys.

– Printouts of maintenance backup logbook, including test restoration, faults, virus scans.

– Folder with warranties, invoices receipts, maintenance agreements.

This practice reserves has right to check individual computer systems history as a precaution to fraud, workplace harassment or breeches of confidence by employees. Inappropriate use of the practices computer systems or breeches 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 the system crash a power failure. This plan encompasses all critical areas of the practices operation 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 and that the practice can continue to operate in the event of a computer failure power outage.

6.1.2 Practice privacy policy

National privacy principle 5 requires a practice to have a document that clearly sets out its policies on handling personal information, including health information.

This document commonly called a privacy policy, is how we handle personal information collected (including health information) and how we protect the security of this information. It must be made available to anyone who asks for it and patients are made aware of this. The collection statement informs patients about how the health information will be used including other organisations to which the practice usually discloses patient information and any law that requires a particular information to be collected. Patient consent to the sharing of patient health information should be provided an early stage in the process of clinical care and patient should be made aware of the collection statement when giving consent to share health information.

In general, quality improvement on or clinical audit activities for the purpose of seeking to improve the delivery of a particular treatment of service will be considered it directly related secondary purpose for information you use disclosure so we do not need to seek specific consent for the use of patients health information, however we include information about quality improvement activities in clinical audits in the practice policy on managing health information. (Refer section 8 accreditation and continuous improvement)

Procedure

We are for our patients about our practices policies regarding the collection management of the personal information via:

– Our new patient information sheet

– New patient forms "consent to share information"

– Verbally if appropriate

Our privacy policy is located in the privacy and procedures manual, at reception.

The privacy policy includes:

– The practices contact details

– 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

– The procedures for patients to gain access to their own health information on request

– The way the practice gains patient consent before disclosing the personal health information to 3rd parties

– The process of providing health information to another medical practice your patience request that – The use of patient health information for quality assurance, research and professional development

– The procedures for informing patients about privacy arrangements

– The way the practice addresses complaints about privacy related matters

– The practice policy for retaining patient health records A collection statement sets up the following information:

– The identity of the practice and how to contact it - The fact that patients can access their own health information

– The purpose for which the information is collected

– Other organisations to which to practice usually discloses patient health information

– Any law that requires a particular information to be collected e.g. notifiable diseases

– The main consequence for the individual if important health information is not provided prior to a patient signing consent to the release of their health information patients are made aware that they can request a full copy of our privacy policy and collection statement.

6.2 Third party requests for access to medical records/health information policy

Request for third-party access to the medical record should be initiated by either receipt of correspondence from a solicitor or government agency or by the patient completing a patient request for personal health information form. Where a patient request form and signed authorisation is not obtained the practice is not legally obliged to release.

Where requests for access refuse the patient of third party may seek access under relevant privacy laws.

An organisation holds health information, it is in their position or control. If you have received reports or other health information from another organisation such as a medical specialist, you are required to provide access in the same manner as for the record to create. If the specialist has written "not to be disclosed to a third party " or "confidential" on their report. This has no legal effect in relation to requests for access under the health records act. You are also required to provide access to records which have been transferred to you from another health service provider.

Request for access to medical record and associated financial details may be received from various 3rd parties including:

– 1. Subpoena /court order /coroner /search warrant
– 2 relatives /friends / carers
– 3 External doctors and healthcare institutions
– 4 Police/solicitors
– 5 Health insurance companies/workers compensation/social welfare agencies
– 6 Employers
– 7 Government agencies
– 8 Accounts/debt collection
– 9 Students (medical and nursing)
– 10 Research/ Quality assurance programs
– 11 Media
– 12 International
– 13 Disease registers
– 14 Telephone calls

Requests from patients to access their own medical records onto the privacy legislation is discussed and 6.3

We only transfer or release patient information to a third party once the consent to share information has been signed in a specific cases informed patient consent maybe sort. Where possible de-identified information is sent.

Our practice team can describe the procedures for timely, authorised and secure transfer of patient health information in relation to valid requests.

Procedure

The practice team can describe how we correctly identify a patient is in three patient identifiers, name, date of birth, address or gender, to ascertain we have the correct patient record for entering, action or releasing anything from that record.

Patient consent for the transfer of health information to other providers or agencies is obtained in the first was and retained on file in anticipation of where this may be required.

As a rule a patient information as to the release with third-party lest the request is made in writing and provides evidence of a signed authority to release the requested information, to either the patient directly or third party. Where possible de-identified data is released.

Written request should be scanned into a patient's medical record. Request should be forwarded to the designated person within the practice for follow-up.

Requested records are to be reviewed by the treating medical practitioner or principal Doctor prior to release with third party. Having satisfied criteria for release (including the patients we can centre where appropriate re-authorisation from the treating doctor), then the practice may specify charge to be incurred by the patient or third party, to meet the cost of the time spent preparing a record photocopying record.

The practice retains a record of all requests for access to medical information including transfers to other medical practitioner. These are scanned into the patient's record. With hardcopy medical records are sent to patients, or third parties, copies of forwarded, not original documentation wherever possible. If originals are required copies are made in case of loss, and these are posted by registered post.

Security of any health information requested is maintained when transferring requested records and electronic data transmission of patient information from our practice is in a secure format.

Subpoena, court order, current search warrant

Scanned a question to patients notes after being notated by the responsible note the date of court case and date request received in the medical record. Depending on whether a physical electronic copy of the record is required following procedure as described above. Refer also to section 8 "management of potential medical defence claims."

On occasions a member of staff is required to accompany the medical record to call alternatively a secure career service may be adequate. If the original is transported. Ensure a copy is made in case of loss of the original during transport. Ensure that the record is returned after review by the court.

Relatives friends

Patient may authorise another person to be given access if they have a legal right in the sign authority. See 6.3 patient requests for personal health information. See also NPP2 Use and disclosure.

In 2018 and the Australian law reform commission recognised that the disclosure of information to a person responsible for an individual" can occur within current privacy law. If a situation arises where a carer is seeking access to a patient's health information, practices are encouraged to contact the medical defence organisation for advice before such access is granted.

Individual records are advised for all family members but especially for children whose parents have separated where care must be taken that sensitive demographic information relating to either parent is not recorded on the demographic sheet. Significant court orders relating to custody and guardianship should be recorded as another on the children's records.

External doctors and healthcare institutions

Direct the query to the patients doctor and/or practice manager/principal doctor

Police/Solicitors

Police and solicitors must obtain a case specific sign patient consent or subpoena/ court order or search warrant for release of information. The request is directed to the doctor

Health insurance companies /workers compensation /social welfare agencies

Depending on a specific circumstances information may be need to be provided. Is recommended that these requests are referred to the doctor

It is important that organisations tell individuals what could be done with their personal health information and if it is within the reasonable expectations of the patient and personal health information may be disclosed. Doctors may need to discuss such request with the patient and perhaps the medical defence organisation

Employers

If the patient has signed consent to release information for a pre-employment questionnaire or similar report then direct the request to the treating doctor.

Government Agencies

Medicare/Dept. Vet Affairs

Depending on the specific circumstances information may need to be provided. It Is recommended that doctors discuss such issues with the medical defence organisations.

State Registrar of Births Deaths Marriages

Death certificates are usually issued by the treating doctor.

Centrelink

There are a large number of Centrelink forms (treating doctors reports) which are usually completed in conjunction with the patient consultation.

Accounts/Debt Collection

The practice must maintain privacy of patient's financial accounts. Accounts are not stored on the physical in areas when members of the public have unrestricted access. Accounts must not contain any clinical information. Invoices and statement should be reviewed pride affording to 3rd party such as insurance companies of debt collection agency's. Outstanding account queries are just you should be directed to the practice manager.

Researchers/Quality Assurance Programs

Where the practice seeks to participate in human research activities and all continuous quality improvement CQI activities, patients anonymity will be protected. The practice will also second retain a copy patient consent to any specific data collection for research purposes. Research requested to be approved by the practice manager must have approval from human research ethics committee (HREC) constituted under the NH&MRC guidelines. A copy of this approval will be retained by the practice.

Please direct all inquiries to the practice manager. Staff must not release any information unless it has been authorised by the practice manager and patient consent has been obtained. International. Where a patient consent is provided that information may be sent overseas however the practice under no obligation to supply any patient information upon receipt of an international subpoena.

Practice accreditation is recognised peer review process and the reviewing of medical records for accreditation purposes has been deemed as a "secondary purpose" by the office of the federal privacy commissioner. As a consequence, patients are not required to provide consent.

Patients are advised of the ways in which the health information may be used (including for accreditation purposes) via the practice information brochure.

Media

Please direct all inquiries the practice manager. Staff must not release any information unless it has been authorised by the practice manager and patient consent has been obtained.

International

Whether patient consent is provided than information may be sent overseas however the practices under no obligation to supply any patient information upon receipt of an international subpoena.

Disease registers

This practice may be required by law to submit any infectious diseases to various disease-specific registers (including cervical).

Telephone calls

Requests for patient information are to be treated with care and no information is to be given out without adherence the following procedure: take a telephone number, name and address of the person calling in for this onto the treating doctor, practice manager where appropriate.

6.3 Patients request for access to personal health information under privacy legislation policy

Patients at this practice have the right to access the personal health information medical record under legislation. Commonwealth privacy amendment privacy sector act 2000.

(The HRA gives individuals a right of access to the personal health information held by any organisation in the private sector in accordance with health privacy principles 6 HPP 6.) This principal obliges health service providers and other organisations that hold health information about a person to get that access to the health information on request, subject to certain exceptions to the payment of fees if any.

Public sector organisations continue to be subject to the Freedom of information act 1982.

This practice complies with both laws and the national and health privacy principles (NPP's and HPP's) adopted therein. See summary headings of principles in this section. Both acts give individuals the right to know what information are private sector organisation holds about them, the right to access this information and to also make corrections if they consider data is incorrect.

National Privacy Principles

NPP6 Relates to access and correction of personal information held by an organisation about an individual, by that individual.

NPP7 The use of identifies assigned by Commonwealth agency.

NPP8 Individuals have the option of not identifying themselves when entering transactions with organisations. Regulates the transfer of personal information held by an organisation in Australia.

NPP9 Regulates the transfer of personal information held by an organisation Australia.

NPP10 Limits on when an organisation is permitted to collect sensitive information.

For national privacy principles available at www.privacy.gov.au. As adopted within Commonwealth privacy amendment private sector at 2000.

We have a privacy policy in place that sets out how to manage health information and the steps and individual must take to obtain access to their health information. This includes the different forms of access and the applicable timeframes and fees.

Reports by specialists

This information forms part of the patient's medical record, hence axis is permitted under privacy law.

Diagnostic results

This information forms part of the patient's medical record, hence access is permitted under privacy law.

Note: Amendments to the privacy act apply to information collected after 21 December two okay one, however they also apply to data collected prior to this date provided it is still in use and readily accessible. We respect an individual's privacy and allow access to information via personal viewing in a secure private area. The patient may take notes of their content of their record or maybe given a photocopy of the requested information. The practitioner may explain the contents of the record to the patient if required. An administrative charge may be applied, at the practitioners discretion and in consultation with the privacy officer, e.g. for photocopying record x-rays and for staff time involved in processing request.

Procedure

Notices displayed in a waiting room advising patience and others of the right to access and of our commitment to privacy legislation compliance. Release of information is an issue between the patient to the doctor. Information will only be released according to privacy laws and doctors discretion. Requested records are reviewed by the medical practitioner prior to the release of the written authorisation obtained.

Request received

When our patients will request access to their medical record and related personal information held at this practice, we document each request an endeavour to assist patients in granting access, where possible and according to the privacy legislation. Exemptions to access will be noted and each patient or legally nominated representative, will have their identification checked prior to access being granted.

A patient may take a request verbally at the practice via telephone or in writing via fax or letter. No reason is required to be given. The request is referred to the patients doctor or delegated privacy officer a request for personal health information form was completed to ensure correct processing this information is kept at reception. Once completed a record of the request form is scanned into the patient's record no information is given until the request is agreed by the practice manager.

Request by another not patient

An individual may authorise another person to be given access, if they have the right for example legal guardian and if they have a signed authority. Under NPP2 Use & Disclosure, a person responsible for the patient including a partner, family member, care guardian, a close friend if that patient is incapable of giving or communicating consent, may apply for and be given access for appropriate care and treatment or for compassionate reasons. Identity validation applies.

The privacy act defines a person responsible as a parent of individual child or sibling of the individual who is at least 18 years old spouse of the factory spouse a relative at least 18 years old and a member of the household, guardian or a person exercising and enduring power of attorney granted by the individual that can be exercised for that person's health a person who has an intimate relationship with the individual or a person nominated by the individual in case of emergency.

Children

When a young person is capable of making their own decisions regarding their privacy they should be allowed to do so according to federal privacy commissioners privacy guidelines. The doctor could discuss the child's record with their parent. Each case is dealt with subject to the individual circumstances. A parent will not necessarily have the right to their child's information.

Deceased persons

A request for access may be allowed for deceased patients legal representative if the patient has been deceased for 30 years or less and all the other privacy law requirements have been met. REF: Sec 28 health records act. No mention is made of deceased patient access in, of privacy legislation.

Acknowledge request

Each request is acknowledged with the letters sent to the patient confirming request has been received. Send the letter within 14 days are seen as recommended by the National privacy commissioner. Acknowledgement will include a statement concerning charges involved in processing the request.

Fees charged

Discuss with the individual or information they want access to and the likely fees before undertaking their request for access.

The fees which an organisation can charge for providing access must not be excessive and must not apply to the mere lodgement for a request of access. National privacy principle in PPE 6.4 aims to prevent organisations from using excessive charges to discourage individuals from making requests for access to the medical records. If an organisation incur substantial costs a meeting request for access, then the organisation could charge a reasonable fee to make the administrative costs involved. For example an organisation could recover some of the costs of photocopying all the staff time involved.

Current fact sheets about fees can be downloaded from www.privacy.gov.au/publications/index.HTML#1.

Collate & Assess information.

Arrange for the treating doctor or practice principle to access the computer record. Refer to the patient request form to help identify what information is to be given to the patient. Data may be held under privacy legislation NNPP6 access and correction for the following reasons.

– Where access would pose a serious threat to the life of health of an individual.

– Where the privacy of others may be affected

– If a request is frivolous or vexatious

– If information relates to existing or anticipated legal proceedings

– If Access would prejudice negotiations with the individual

– If access would be unlawful

– Where denying access is required or an authorised by law.

See National privacy principles in full for comprehensive list of exclusions.

Access denied

Reasons for denied access must be given to the patient in writing. Note these on a request form. In some cases refusal of access maybe impart waiting for.

Use of intermediary when Access denied

If request for access is denied an intermediary, make operate as a facilitator to provide sufficient access to meet the needs of both the patient and the doctor.

Provide access

Personal health information may be accessed in the following ways:

– view and inspect information

– you inspect talk to contents with Dr

– take notes

– obtain a copy (can be photocopied or electronic printout from computer.)

Check Identity of Patient

- Ensure a visible form of ID is presented by the person seeking access e.g. drivers license, passport other photo iD. Note details on request form
- Does the person have the authority to gain access? Check age, legal guardian documents; is person authorised representative.

If the patient is viewing the data, supervise each viewing so the patent is not disturbed and no data goes missing. If a copy is to be given to the patient ensure all pages are checked and this is noted in the request form. If the doctor is to explain the contents to patient then ensure an appropriate time is made.

Requests to Correct Information

A patient may ask to have their personal health information amended if he/she considers that is not up to date, accurate and complete (NPP 6.5/6/6).

Our practice must try to correct this information. Corrections are attached to the original health record. Where there is a disagreement about whether the information is indeed correct, our practice attached a statement to the original record outlining the patients claims.

Time Frames

Acknowledge request in 14 days. Complete the request in 30 days.

6.3.1 Privacy Officer

Policy

This practice has a designated Privacy Officer who implements and monitors adherence to all privacy legislation in this practice.

The privacy officer acts as a liaison for all privacy issues and patient requests for access to their personal health information.

If staff members have any queries concerning privacy law: i.e Commonwealth Privacy Act – Privacy Amendment (Private Sector) Act 2000, or Victorian Health Records Act 2001 then refer to the Privacy Officer.

The privacy officer is responsible for ensuring compliance with relevant Privacy principles and legislation and for developing and maintain our written protocols. The privacy officer liaises with the person responsible for computer security and systems. Our designated representative is Dr Rachel Earl.

6.3.2 Privacy Audit

Policy

From time to time or in the event of any issues or complaints relating to privacy matters, this practice conducts a review of privacy policies and procedures.

Procedure

The Privacy officer reviews the following items:

- What is the primary purpose of this practice?
- What data do we collect and document? NPP1/HPP1
- How do we store this information NPP5?
- What data do we disclose and to whom? NPP2
- When and how do we obtain patient's consent? NPP2/HPP2
-

Information is collected via electronic storage devices and issues discussed with GP and staff to gain the most current information.

National and state privacy laws are referenced with any updates being noted and acted upon.

Policy manual, Patient Access Forms/Register, Brochures and Poster

At this time the Practice policy and procedure manual may be reviewed and updated for privacy terms, if not already done.

Forms related to "Patient Access to Health Information" including request for access and access register forms can be also be reviewed at this time.

Detailed patient privacy information, stating our practice privacy policy in general as per privacy legislation is reviewed and updates as necessary. Obtain additional copies in English or other languages or re-print as needed.

Ref: Guidelines in Privacy in the Private Health Sector; Office of the Federal Privacy Commissioner Oct 2001.

To assist with managing any complaints regarding privacy breeches. The Complaints Management Handbook for Health Care Services – AUSTRALIAN COUNCIL FOR SAFETY AND QUALITY IN HEALTH CARE (July 2005) www.safetyandqaulity.health.wa.gov.au/docs/complaints/ACSQHC%20compintmgmtbk.pdf

6.4 Medical records and Administration Systems

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

Our practice uses Best Practice software for the storage and management of patient health information.

6.4.1 Creating a New Record

Once patient name, address date of birth and related demographic details are received by reception with this information into the patient record.

Computerised patient records are only accessed by authorised doctors and staff via secure login/password.

6.4.3 Filing Reports (Pathology, X-Ray, Ultrasound, Consultants etc)

Results are received electronically and are checked by the referring doctor daily, and the appropriate action box is marked. The doctor will ensure that the action is completed.

6.4.4 Errors in Medical record

Corrections in the electronic record should be recorded by referring to the date of the original entry and the associated amendment.

Refer to NPP6/HPP6 Access & Correction which refers to the patients' rights to have their personal health information amended if he/she can establish that it is not accurate, complete, misleading or up to date.

6.4.5 Allergies and Alerts

Alert notification may be required for allergic responses, drug reaction, and previous aggressive behavior or guardian/custody arrangements.

It is practice policy to ensure that all patients have their allergenic status recorded especially any allergies to medications to facilitate safer prescribing. In computer based records "no known allergies" is recorded in the absence of any allergies to note.

Alert notifications are documented in the electronic medical record Health Summary.

6.4.6 Backup of electronic medical records

In order to avoid lengthy down time, disruption and medico-legal issues frequent backups are essential and form a critical component of the practice disaster recovery plan. A formal policy for the back up pf the practice computer systems in place.

6.4.7 Retention of Records and Archiving

Patient Health Records must be kept until the patient is 25 years of age, if a child, or pregnancy management (eg fetus) or a minimum of 7 years following the last year of the patients attendance whichever is greater.

Inactive electronic patient records are retained indefinitely or as stipulated by the relevant national state or territory legislation. Patients are marked as inactive if they have not attended the practice 3 or more time in the past 2 years.

Patients accounts records are also retained for a minimum of 7 years.

Records of drugs of addiction and administration must be retained for a minimum of 3 years. Sterilisation records and monitoring are retained as per patient health records.

Records of patients that have been sought for legal purposes are retained as above.

The practice has a process in place to allow for the timely identification, of information to be culled, stored at this time.

Procedure

Privacy will be maintained during the destruction process to ensure information contained in the records is not divulged or seen by unauthorised persons.

6.4.8 Transfer of Medical Records

Policy

Transfer of medical records from this practice can occur in the following:

- For medico-legal purposes eg record is subpoenaed to court
- When a patient asks for their medical record to be transferred to another practice due to moving residence or other reasons.
- Where an individual medical record is requested from another source.
- Where the doctor is retiring, and the practice is closing.

Our practice team can describe the procedures for timely authorised and secure transfer of patient information to other providers in relation to valid requests.

Requests for transfer of medical records for medico legal reasons

Refer to 6.2 3rd Part Requests for Access to medical Records – Health Information

Receiving a request to transfer medical records to a patients new clinic

In accordance with state and federal privacy regulations a request to transfer medical records must be signed by the patient giving us authority to transfer their records.

The request form should contain:

- The name of the receiving practitioner or practice
- The name, address (both current and former if applicable) and date of birth the patient whose record is required.

When fulfilling a request, this practice may choose to either:

- Prepare a summary letter (via clinical software) and include copies of relevant correspondence and results pertinent to the ongoing management of the patient.
- Make a copy of the medical record and dispatch the copy to the new practice retaining the original on site for a minimum of 7 years.

The requesting clinic is advised if we propose to transfer a summary or a copy of the full medical record. If they have a preference the format can be negotiated, or they can choose not to proceed with the transfer and seek a copy through a separate access request.

If there is going to be any expenses related to the transfer the requesting clinic is advised prior to sending the medical records and once the fee has been paid we process the request as soon as possible. Any charged must not exceed the prescribed maximum fee.

The patients signed request form is scanned into the patients record and a notation that the patient has transferred is made on the medical record. Include the name and address of the new Practice and the dispatch details (eg registered post or confidential courier or in electronic form).

Electronic data transmission of patient health information from our practice is in a secure format. Note: There are a number of ways the information can be transferred, depending on the request form and clinic: via registered post, encrypted email (computerized record) or if the practice is releasing copies of the entire record and the patient requests access (Health records Act), the practice may wish to make an appointment tie with the patient to offer an appropriate explanation and counsel from the GP or as an alternative may choose to supply a summary of the history.

All reasonable steps are taken to protect the health information from loss and unauthorised disclosure during the transfer,

This practice does not allow individual to collect the file and take to their new provider.

Making a request for a patient medical record from another source

Access to a new patients previous record can assist with maintaining the continuity of care for the patient.

When requesting records from another clinic a standard Request for Transfer of Medical Records form should be used. This should contain:

- The patient details
- The patient should identify name, address (both current and former if applicable) and date of birth
- The name of the doctor making the request
- The request for the transfer of patient files should be authorised by the patient

If the files will be requested electronically, specific details of the format needs to be included such as HTML, or PDF.

If the clinic advises you the patients are likely incur an out of pocket expense related to the transfer please advise the patient proper to accepting the transferred medical records.

When a Doctor is retiring and the practice is closing

The correct handling patient information on the closure of a practice is available at www.
privacy.gov.au/materials/types/guidelines/view/6517