Privacy Policy

This practice is bound by *The Privacy Act 1988 (Comm.)* and National Privacy Principles, and also complies with the *Health Records Act 2001 (Vic.)*.

'Personal health information' is defined as a 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, Leon Morgiewicz with primary responsibility for the practice's electronic systems, computer security and adherence to protocols as outlined in our Computer Information Security Policy. This responsibility is documented in the Position Description. Tasks may be delegated to others and this person works in consultation with the privacy officer.

Access will be provided in accordance with the guidelines set out in the Health Records Regulations 2002. If a patient requires access to their personal information, they are to complete a Privacy Release Form, which will be reviewed and actioned by the Practice Manager/Privacy Officer. A fee may be charged to a patient requesting a copy if their medical records.

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.

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 patient's 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 that 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/her privacy clause contained with the employment agreement which is signed upon commencement of employment at this Practice.

Personal health information is kept where staff supervision is easily provided and kept out of view and access by the public. Scanning of patient files is to be undertaken in the 'back office' under supervision of the Practice Manager, ensuring optimum confidentiality when entering and allocating correspondence.

Practice computers and servers comply with the RACGP computer security checklist and we have a sound back up system and a contingency plan to protect the practice from loss of data.

Care should be taken that the general public cannot see or access computer screens that display information about other individuals. In the Administrative department, care is taken to ensure computers are turned to an angle that is not easily visible to patients, and confidential phone calls are handled away from the reception desk. Within the clinical sector, both doctors and nurses take great care to ensure all patient files are closed before a new patient can enter, and all urgent phone calls are engaged with optimum confidentiality. If a phone call cannot be managed confidentially within the consult room, a general practitioner or nurse may ask the patient to leave, or direct the phone call to a vacant room to continue the phone call privately

Members of the practice team have different levels of access to patient health information. To protect the security of health information, GPs and other practice staff do not give their computer passwords to others in the team unless given permission to do so by the Practice Manager, Mr Leon Morgiewicz.

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 a secure, locked bin from a local document destruction service:

- Cleanaway
- Phone: 02 60244590

All confidential information must go into the locked blue bin for destruction, located in the staff toilets. It is the responsibility all staff members to alert the Practice Manager when the bin is mostly full to allow adequate time for collection and destruction.

1. Correspondence

Incoming patient correspondence and diagnostic results are received via Australia post, and are opened by either a senior receptionist or the administrative trainee in the 'back office'.

Items for collection or postage are left in a secure area within the 'back office', in direct line of sight of the Practice Manager. It is the duty of the office trainee to hand deliver this mail to the post office, and return the receipt to either the Practice Manager or Senior Receptionist upon return. Items deemed confidential by either the office manager or practice manager will be

marked accordingly, and measures will be taken to ensure appropriate postage or delivery (for example, registered postal mail through Australia Post, or personal delivery by the Practice Manager for personal files to an alternate medical practice within appropriate driving distance).

2. Facsimile

Facsimile, printers and other electronic communication devices in the practice are located in a central location, accessible to the general practitioners and other staff who have been adequately trained for the items use.

All faxes containing confidential information are sent to fax numbers after ensuring the recipient is the designated receiver. It is integral that all confidential information has a cover sheet, including the name of the addressee, fax number, a brief message and the word "Confidential" displayed prominently.

It may be necessary to call the recipient 5-10 minutes after the fax was transmitted, to ensure its receipt.

Faxes received are managed according to incoming correspondence protocols

3. Emails

Emails are sent via various nodes and are 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.

4. Patient Consultations

Patient privacy and security of information is maximised during consultations by closing consulting room doors. All Examination couches, including those in the treatment room, have curtains or privacy screens equipped for those wishing to utilise extra privacy.

When, consulting, treatment room or administration office doors are closed prior to entering staff should either knock and wait for a response or alternatively contact the relevant person by internal phone or email.

It is the doctor's/health care professional's responsibility to ensure that prescription paper, medical records and related personal patient information is kept secure, if they leave the room during a consultation or whenever they are not in attendance in their consulting/treatment room.

5. 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.

When a written request is received, the Office Manager has permission to access and allocate medical records as necessary.

Both active and inactive patient health records are kept and stored securely.

Our Practice has been fully computerised for over 11 years and physical medical records are rarely if ever accessed.

6. Computerised Records

Our practice is considered virtually 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.

Although paper files exist on site, they are no longer actively used and are in the process of undergoing archiving and destruction as per Australian Government Privacy Legislation.

7. Computer Information Security

8. Policy

Our 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.

The Practice Manager, Mr Leon Morgiewicz, 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 medico legal reasons, and to provide evidence of items billed in the event of a Medicare audit, staff, especially nurses 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 authorisation
- computers have screensavers or other automated privacy protection devices are enabled to prevent unauthorised access to computers
- servers are backed up and checked at frequent intervals, 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 licence keys
- logbooks/print-outs of 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 Practices Computer Systems or 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 and that the practice can continue to operate in the event of a computer failure or power outage.

Procedure:

Our Complete DR plan is located on the quality drive of the file server.

Our disaster Box stocked with items to enable the practice to operate in the event of a power failure is located at the front desk

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

9. Practice 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.

This document, commonly called a privacy policy, outlines 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 their health information will be used including other organizations to which the practice usually discloses patient health information and any law that requires the particular information to be collected. Patient consent to the handling and sharing of patient health information should be provided at an early stage in the process of clinical care and patients should be made aware of the collection statement when giving consent to share health information.

In general, quality improvement or clinical audit activities for the purpose of seeking to improve the delivery of a particular treatment or service would be considered a directly related secondary purpose for information use or disclosure so we do not need to seek specific consent for this use of patients' health information, however we include information about quality improvement activities and clinical audits in the practice policy on managing health information.

Procedure

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

- Brochures in the waiting area
- Our patient information sheet
- New patient forms- "Consent to share information"
- Verbally if appropriate

The Albury-Wodonga Family Medical Centre collects and holds personal health information about our patients. This information is collected so that we may properly assess, diagnose, treat and be proactive in our patient's health care needs. All members of the professional team involved in patient care may have access to patient's personal information. Some information we collect is in order to comply with our legal obligations such as Mandatory Reporting or Accreditation. This means we may use and disclose information that patients provide in the following ways;

- Disclosure to others involved in patient healthcare, including treating doctors, pathology services, radiology services and other specialists outside this medical practice. This may occur through referral to other doctors or medical tests and in the reports or results returned to us following the referral.
- Disclosure to enable recording on medical registers (ie diabetes or pap smear register)
- Administrative purposes in running our medical practice including our insurer or medical indemnity provider, quality assurance and accreditation bodies.
- Billing purposes including providing information to a patient's health insurance fund, the Health Insurance Commission (Medicare) and other organizations responsible for the financial aspects of a patients care.
- In most cases, the required information will be obtained directly from patients or their treating doctor.

Our goal is to ensure that patient information is accurate, complete and up-to-date. To assist with this we request patients inform us of any change in their personal information. We will use all reasonable efforts to ensure patient information is accurate, complete and up-to-date.

We will take all reasonable steps to protect the security of personal information that we hold. This includes appropriate measures to protect electronic materials and materials stored and generated in hard copy. We do not contract our data storage or processing functions.

Patients are not obligated to provide their personal information. Should a patient choose not to provide the Albury-Wodonga Family Medical Centre with their personal details (e.g. name and address) we may not be able to provide the patient with our full range of services (e.g. recalls).

Prior to a patient signing consent to the release of their health information patients are made aware they can request a full copy of our privacy policy and collection statement.

Patient consent for the transfer of health information to other providers or agencies is obtained on the first visit. A copy of our consent form is included in section 6, Forms, Templates and Checklists.

Once signed, this form is scanned into the patient's record and its completion tracked and processed by administration staff.

10. 3rd Party Requests for Access to Medical Records/Health Information

Policy

Requests 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 or and signed authorisation is not obtained the practice is not legally obliged to release.

Where requests for access are refused, the patient or third party may seek access under relevant privacy laws.

Organizations 'hold' health information if it is in their possession or control. If you have received reports or other health information from another organization such as a medical specialist, you are required to provide access in the same manner as for the records you 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. Staff is also required to provide access to records, which have been transferred to you from another health service provider.

Requests for access to the medical record and associated financial details may be received from various Third Parties including:

1. Subpoena, court order, coroner, search warrant
2. Relatives, Friends, carers
3. External doctors & Health Care 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& Nursing)
10. Research, Quality Assurance Programs
11. Media
12. International
13. Disease registers
14. Telephone Calls

We only transfer or release patient information to a third party once the consent to share information has been signed and in specific cases informed patient consent may be sought.

Applicable practice team members can describe the procedures for timely, authorized and secure transfer of patient

Procedure

The practice team can 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, actioning or releasing anything from that record.

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

As a rule no patient information is to be released to a 3rd Party unless the request is made in writing and provides evidence of a signed authority to release the requested information, to either the patient directly or a third party.

Written requests should be noted in the patient's medical record. Requests should be forwarded to the designated person within the practice for follow-up.

Requested records are to be reviewed by the treating medical practitioner and Practice Manager prior to their release to a third party. Where a report or medical record is documented for release to a third party, having satisfied criteria for release, (including the patients written consent and where appropriate written authorization from the treating doctor), then the practice may specify a charge to be incurred by the patient or third party, to meet the cost of time spent preparing the report or photocopying the record.

The practice retains a record of all requests for access to medical information including transfers to other medical practitioners.

Where hard copy medical records are sent to patients or 3rd Parties copies are forwarded not original documentation wherever possible. If originals are required copies are made in case of loss.

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

Subpoena, Court Order, Coroner Search Warrant

Note the date of court case and date request received in the medical record. Depending on whether a physical or electronic copy of the record is required follow procedures 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 court or alternatively a secure courier service may be adequate. If the original is to be transported, ensure a copy is made in case of loss or damage to the original during transport. It is integral that the Office Manager or Practice Manager ensure that the court returns the record after review.

Relatives or Friends

A patient may authorise another person to be given access if they have the legal right and a signed authority. See 6.3 Patient Requests for Personal Health Information and NPP2 Use & Disclosure.

In 2008 the Australian Law Reform Commission recognised that 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 their 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 partner is not recorded on the demographic sheet. Significant court orders relating to custody and guardianship should be recorded as an alert on the children’s records.

External Doctors & Health Care Institutions

Direct the query to the patient’s doctor and or the practice manager/principal doctor as applicable, and fill out the required paperwork as per both organisations policy and procedures

Police or Solicitors

Police and solicitors must obtain a case specific signed patient consent (or subpoena, court order or search warrant) for release of information. The request is then directed to the doctor applicable, or Practice Manager will carry out all decisions made.

Health Insurance Companies, Workers Compensation and Social Welfare Agencies

Depending on the specific circumstances, information may need to be provided. It is recommended that these requests be referred to the Doctor, and all issues noted and passed on to either the Practice Manager as applicable.

It is important that organizations tell individuals what could be done with their personal health information and if it is within the reasonable expectation of the patient then personal health information may be disclosed. Doctors may need to discuss such requests with the patient and perhaps their medical defense organization.

Employers

It is integral that the patient signs an agreement allowing the release of information to an employer or employing firm, especially in the case of pre-employment medicals.

In the case of general appointment enquiries, an employer is not able to receive any information about staff health unless the patient has consented in writing.

11. Government Agencies

Medicare/Dept. Veterans Affairs

Depending on the specific circumstances, information may be need to be provided to agencies such as Medicare or the Department of Veterans Affairs (DVA). It is recommended that doctors and practice management discuss such issues with the medical defence organisations.

State Registrar of Births, Deaths & Marriages

The treating doctor usually issues death certificates as required for deceased patients.

Centrelink

There are a large number of Centrelink forms (treating doctor's reports), which are usually completed in conjunction with the patient consultation. The patient will usually provide consent for release of information, and this is noted both in the consultation notes and on the form itself.

12. Accounts and Debt Collection

The practice must maintain privacy of a patient's financial accounts. Accounts are currently stored on the practice billing software, 'Best Practice', and access is limited to the public through computer confidentiality practice

Accounts must not contain any clinical information, unless patient consent is provided (for example, Work Cover Claim details). Invoices and statements should be reviewed prior to forwarding to third parties such as insurance companies or debt collection agencies.

Outstanding account queries or disputes should be directed to the practice manager or principal.

13. Students (Medical & Nursing)

This practice does participate in medical/nursing student education at present due to size constraints. On completion of renovations in 2016, this will be reviewed

The practice acknowledges that some patients may not wish to have their personal health information accessed for educational purposes. The practice always advises patients of impending student involvement in practice activities and seeks to obtain patient consent accordingly. The practice respects the patient's right to privacy.

14. Researchers and Quality Assurance Programs

Where the practice seeks to participate in human research activities and/or continuous quality improvement (CQI) activities, patient anonymity will be protected. The practice will also seek and retain a copy of patient consent to any specific data collection for research purposes.

Research requests are to be approved by the Practice Principal/ practice partners and must have approval from a Human Research Ethics Committee (HREC) constituted under the NH&MRC guidelines. A copy of this approval will be retained by the practice.

Practice accreditation is a 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.

15. Media

Please direct all enquiries to Practice Manager or Principal. Staff must not release any information unless it has been authorised by the Practice Manager or Principal and patient consent has been obtained (if relevant)**.**

16. International

Where patient consent is provided, then information may be sent overseas. As an Australian practice, we are under no obligation to supply any patient information upon receipt of an international subpoena.

17. Disease Registers

This practice submits patient data to various disease specific registers (cervical, breast bowel screening et cetera) to assist with preventative health management.

Consent is required from the patient, with the option of opting in or opting out. Patients are advised of this via pamphlets in the waiting area and through their General Practitioner or Registered Health Professional.

18. Telephone Calls

Requests for patient information are to be treated with care and no information is to be given out without adherence to the following procedure:

1. Take the telephone number, name (and address) of the person calling
2. Forward this onto the treating doctor/principal or Practice Manager where appropriate

19. Patients Request for Access to Personal Health Information under the Privacy Legislation

Policy

Patients at this practice have the right to access their personal health information (medical record) under legislation: Commonwealth *Privacy Amendment (Private Sector) Act 2000* and the *Health Records Act 2001 (Victoria) (also known as the 'HRA').*

The 'HRA' gives individuals a right of access to their personal health information held by any organization in the private sector in Victoria in accordance with Health Privacy Principle 6 (HPP6). This principle obliges health service providers and other organizations that hold health information about a person to give them access to their health information on request, subject to certain exceptions and the payment of fees.

Public sector organizations continue to be subject to the *Freedom of Information Act 1982*.

This practice complies with both laws and the National and Health Privacy Principles *(NPPs & HPPs)* adopted therein Both Acts give individuals the right to know what information a private sector organization holds about them, the right to access this information and to also make corrections if they consider data is incorrect. Compliance with the access provisions in the *Health Records Act 2001 (Victoria)* will generally ensure compliance with the Commonwealth Privacy Act.

National Privacy Principles:

NPP 1: Collection of personal information by an organization.

NPP 2: How an organization may use and disclose personal information in its possession.

NPP 3: Relates to the quality of the data held by an organization.

NPP 4: Organization must take reasonable steps to make sure the personal information it holds is secure

NPP 5: Requires an organization to be open about what personal information it holds and its policy on the management of personal information.

NPP 6: Relates to access and correction of personal information held by an organization about an individual, by that individual.

NPP 7: The use of identifiers assigned by a Commonwealth Agency

NPP 8: Individuals have the option of not identifying themselves when entering transactions with organizations

NPP 9: Regulates the transfer of personal information held by an organization in Australia

NPP10: Limits on when an organization is permitted to collect sensitive information

As adopted within Commonwealth Privacy Amendment (Private Sector) Act 2000

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

Reports by Specialists

This information forms part of the patient's medical record, hence access 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 21st December 2001, 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 the content of their record or may be given a photocopy of the requested information. A GP may explain the contents of the record to the patient if required. An administrative charge may be applied at the GPs discretion, e.g. for photocopying record, X-rays and for staff time involved in processing request.

Procedure

A notice is displayed in our privacy pamphlet, advising patients and others of their rights of access and of our commitment to privacy legislation compliance. Both reception and administrative staff upon patient request can provide further clarification on privacy policy and procedure.

Release of information is an issue between the patient and the doctor. Information will only be released according to privacy laws and at doctor's discretion.

Request Received

When our patients request access to their medical record and related personal information held at this practice, we document each request and endeavour to assist patients in granting access where possible. 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 make a request verbally at the practice, via telephone or in writing e.g. fax, email or letter. No reason is required to be given. A Request for Personal Health Information must be signed and dated before any information request can be considered. The request is then referred to the Practice Manager for processing.

Once completed, a record of the request is scanned in the patient record on Best Practice.

Request by another (not patient)

An individual may authorise another person to be given access, if they have the right (e.g. legal guardian), and if they have a signed authority from the patient in question. Under *NPP 2 -Use & Disclosure*, a 'person responsible' for the patient (including a partner, family member, care, guardian or 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 the individual, a child or sibling of the individual, who is at least 18 years old, a spouse or de facto spouse, a relative (at least 18 years old) and a member of the household, a guardian or a person exercising an 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

Where a young person is capable of making their own decisions regarding their privacy, they should be allowed to do so according to Federal Privacy Commissioner's Privacy Guidelines. The doctor could discuss the child's record with their parent if under the age of 14 years. Each case is dealt with subject to the individual's circumstances, and a parent will not necessarily have the right to their child's information.

Deceased Persons

A request for access may be allowed for a deceased patient's legal representative if the patient has been deceased for 30 years or less and all other privacy law requirements have been met (*Ref: Sec 28 Health Records Act*). No mention is made of deceased patient's access in Commonwealth privacy legislation.

Acknowledge Request

Each request is acknowledged with a letter sent to the patient, confirming request has been received. The letter is sent within 14 days, or sooner, as recommended by the *National Privacy Commissioner*. Acknowledgment will include a statement concerning charges involved in processing the request.