1.0 Privacy

Policy
All patient information is private and confidentiality of patient information must be maintained at all times. The rights of every patient are to be respected. All information collected by WGPN in providing a health service is deemed to be private and confidential.

WGPN complies with Federal and State privacy regulations including the *Privacy Act 1998*, the *Privacy Amendment (Private Sector) Act 2000* as well as the standards set out in the RACGP Handbook for the Management of Health Information in Private Medical Practice 1st Edition (2002).

Under no circumstances are employees of WGPN to discuss or in any way reveal patient conditions or documentation to unauthorised staff, colleagues, other patients, family or friends, whether at the practice or outside it, such as in the home or at social occasions. This includes patient's accounts, referral letters or other clinical documentation.

General Practitioners and staff are aware of confidentiality requirements for all patient encounters and recognise that significant breaches of confidentiality may provide grounds for disciplinary action or dismissal.

Every employee of WGPN is aware of the privacy policy and has signed a privacy statement as part of their terms and conditions of employment. This privacy statement continues to be binding on employees even after their employment has terminated.

Procedure

All employees of WGPN are issued with the privacy policy and sign a privacy statement as part of their terms and conditions of employment. The policies and procedures of the practice are further explained during the induction of new staff members, and the induction form is signed by the new employee as confirmation that they understand and accept their obligations in relation to patient privacy and the confidentiality of medical information.

1.1 Practice Privacy Policy

Policy
National Privacy Principle 5 requires WGPN 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 organisations to which WGPN 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. (Accreditation and Continuous Improvement)

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

- a sign at reception.
- brochure/s in the waiting area.
- our patient information sheet.
- new patient forms – 'Consent to share information'.
- verbally if appropriate.
- the practice website.

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.

Once signed this form is scanned into the patient's record and its completion noted.

2.0 Privacy and Personal Health Information

Policy

WGPN is bound by the *Federal Privacy Act 1998* and National Privacy Principles, and also complies with the *Victorian Health Records Act 2001*.

'Personal health information' 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 an IT&T Manager with primary responsibility for the practice's electronic systems, computer security and adherence to protocols as outlined in our Computer Information Security policy.

Our Security policies and procedures regarding the confidentiality of patient health records and information are documented and our practice team are 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 patient health record containing all clinical information held by our practice relating to that patient. WGPN ensures the protection of all information contained therein. Our patient health records can be accessed by an appropriate team member when required. We also ensure information held about the patient in different records (e.g. at a residential aged care facility) is available when required.

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 1998*.

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 should be kept where staff supervision is easily provided and kept out of view and access by the public e.g. not left exposed on the reception desk, in waiting room or other public areas; or left unattended in consulting or treatment rooms.

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. (Computer information security)

Care should be taken that the general public cannot see or access computer screens that display information about other individuals. To minimise this risk automated screen savers should be engaged.

Members of the practice team have different levels of access to patient health information. (Refer Compute Information security) To protect the security of health information, GPs and other practice staff do not give their computer passwords to others in the team.

Reception and other Practice staff 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.

Correspondence
Electronic information is transmitted over the public network in an encrypted format using secure messaging software. Where medical information is sent by post the use of secure postage or a courier service is determined on a case by case basis.

Incoming patient correspondence and diagnostic results are opened by a designated staff 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 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 the designated receiver.

Confidential information sent by fax has Date, Patient Name, Description and Destination recorded in a log book.

Check the number dialled before pressing ‘SEND’
Keep the transmission report produced by the fax as evidence that the fax was sent. Also confirm the correct fax number on the report.

Faxes received are managed according to incoming correspondence protocols

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

Emails
Emails are sent 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.

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.

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.

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

It is the doctor's/health care professional's 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 whenever 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 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.

Our patient health records can be accessed by an appropriate team member when required. All record access is password controlled. Both active and inactive patient health records are kept and stored securely.

Computerised Records

Our 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.

2.1 Privacy Officer

Policy

WGPN has a designated the Patient Services Manager as the Privacy Officer who implements and monitors adherence to all privacy legislation in this practice.

The Privacy Officer acts as 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 maintaining our written protocols. The privacy officer liaises with the person responsible for Computer security and systems.

3.0 Privacy Audit

Policy

From time to time or in the event of any issues or complaints relating to privacy matters, WGPN will conduct 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?
- how do we store this information?
- what data do we disclose and to whom?
- when and how do we obtain patient's consent?

Information is collected from hard copy and electronic storage devices and issues discussed with GPs 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 & procedure manual may be reviewed and updated for privacy items, if not already done.

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

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

A general patient privacy wall poster, advising patients of our privacy policy is reviewed and updated as necessary.

Attachment A

WGPN Privacy Policy

The purpose of this document is to outline how the WGPN complies with its confidentiality and privacy obligations. The WGPN will make this Privacy Policy available to anyone who asks for it.

As an organisation, our principal concern is and always has been the health of patients who visit our medical centre. A high level of trust and confidentiality is required to ensure the confidence of the patients we serve.

From the 21st December 2001, the Privacy Amendment (Private Sector) Act 2000 extended the operation of the Federal Privacy Act 1988 to include the private health sector throughout Australia. Going forward, patients will be assured that their privacy will be protected when visiting our practice; that the information collected and retained in our patient records is correct and up-to date; and that they can access their information for review.

While the new legislation will serve to complement our existing culture of confidentiality and our already established professional practice obligations and to ensure best practice.

No exceptions under the Privacy Act apply to personal information that we hold or to any of our acts or practices.

Collection, Use & Disclosure

We recognise that the information we collect is often of a highly sensitive nature and as an organisation we have adopted the highest privacy compliance standards relevant to ensure personal information is protected.

We are a service company to the medical practitioners who provide services at WGPN. For administrative and billing purposes, and to enable the patient to be attended by other practitioners in our practice, patient information is shared between the practitioners who attend a patient.

We (on behalf of) and the practitioners may collect personal information (including health information) regarding patients for the purpose of providing medical services and treatment to patients. Personal information collected will generally include: the patient's name, address, telephone number and Medicare number; health care fund; current drugs or treatments used

by the patient; previous and current medical history, including where clinically relevant a family medical history, and the name of any health service provider or medical specialist to whom the patient is referred, copies of any letters of referrals and copies of any reports back.

We may access information:

- provided directly by the patient;
- provided on the patient's behalf with the patient's consent;
- from a health service provider who refers the patient to medical practitioners
- from health service providers to whom patients are referred.

Personal information collected by us may be used or disclosed:

- for the purpose the patient was advised of at the time of collection of the information by us;
- as required for delivery of the health service to the patient;
- as required for the ordinary operation of our services (i.e. to refer the patient to a medical specialist or other health service provider);
- as required under compulsion of law; or
- where there is a serious and imminent threat to an individual's life, health, or safety; or
- a serious threat to public health or public safety.

Other than as described in this Policy or permitted under the National Privacy Act, WGPN uses its reasonable endeavours to ensure that identifying health information is not disclosed to any person.

We keep health information for a minimum of 7 years from the date of last entry in the patient record (unless the patient was a child in which case the record must be kept until the patient attains or would have attained 25 years of age). This is because we are required to maintain such records under some laws.

Because of the sensitive nature of the information collected by us to provide its services, extra precautions are taken to ensure the security of that information. Our electronic files are password-protected on several levels, and the computer backup tapes are stored offsite.

We require all our employees and contractors to observe obligations of confidentiality in the course of their employment/contract. We require independent contractors to sign a confidentiality undertaking.

Medical practitioners who provide services at our practices may refer patients to the following services:

- pathology services
- radiology services;
- public hospitals;
- private hospitals;
- day procedure centres;
- specialist medical practitioners and other health providers involved in the relevant patient's care which may include surgeons, nurses, occupational therapists, pharmacists, physiotherapists, psychologists, dieticians, audiologists, podiatrists and the ambulance service.

Secondary purposes which are directly related to the primary purpose of collection for which we may use or disclose personal information may be for quality assurance, training, billing, liaising with government offices regarding Medicare entitlements and payments and as may be required by our insurers.

We also collect information about the medical practitioners who provide services at our practices. This information is collected directly from or with the agreement of the medical practitioner. This information includes the name, address, qualifications and experience of the medical practitioner.

Accessing your information, complaints and obtaining further information

If an individual wishes to:

- complain to us about a breach of privacy; or
- access his or her own information held by us; or
- correct any information held by us concerning his or her own information; or
- find out more about how we deal with personal information, that individual can contact:

The Patient Services Manager, WGPN, 25 Holtfreter Ave, Northam, WA, 6401