

Privacy Policy

APP1 – OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION

“Personal health information” is 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 family/social history, current health issues and future medical care. Personal Health Information also includes your Medicare number, account details and any health information such as medical or personal opinion about a person’s health, disability or health status. It is a formal electronic record and holds information held or recorded on any other medium, eg, letter, fax or electronically or information conveyed verbally.

We collect this health information to help us provide comprehensive, coordinated and continuing whole person medical care for individuals, families and the community. We collect patient information to gain sufficient information to provide for optimal ongoing management of each patient’s health, care and well-being and to ensure practice is viable to continue treating patients.

At your initial attendance, where you are asked to read the sign the consent form, for all or the limited parts that you consent to, you are consenting to the handling and sharing of patient health information as deemed necessary for your comprehensive healthcare. Eg, if you present to an Emergency Department of a hospital and they contact us requesting a copy of your patient health summary to assist them with your medical management.

Other less urgent requests, eg, from Community Health, we will contact you to ask your consent prior to releasing information.

Patient health information is stored in the patient’s electronic file and used for:

- Maintaining current information about patients.
- Updating demographics.
- Accounts – payment, invoicing, follow-up.
- Recall and reminder system.
- Actioning report results.
- Adding to medical record for comprehensive data – results, operation reports, emergency department visits, after hours and home consultations.
- Telephone notes.
- We endeavour to maintain the integrity of personal information by updating demographics at reception as advised by the patient. An Update Your Details Form is located at the front counter. More personal information should be shared with your GP so that our records are up-to-date, complete and relevant.

APP2 – ANONYMITY AND PSEUDONYMITY

We recognise that on occasion patients wish for their consultations to be anonymous and choose to use a pseudonym. We are able to facilitate this if required. However if standard identifiers are not used we will be unable to bulk bill (if the patient is eligible) and a Medicare rebate would not be available if a private patient. This would also be the case with any other allied health care services, such as pathology or imaging that we refer you to under your choice of anonymity or pseudonymity. In terms of recalls or important results or reminders for recommended testing, eg pap smears, a system would be in place to ensure that all information is managed as per our current policies and procedures.

APP3 – COLLECTION OF SOLICITED PERSONAL INFORMATION

If information is required to assist in your medical management, and you are unable to provide this information, we will seek your consent prior to seeking to obtain this information from other sources. We

will only collect sensitive information that is deemed reasonably necessary. We will only collect information by lawful and fair means.

APP4 – DEALING WITH UNSOLICITED PERSONAL INFORMATION

If we receive personal information that we did not solicit, that we could not have collected if we did solicit the information we must, within a reasonable period of time, if lawful to do so, destroy the information or ensure that it is de-identified.

If we collect personal information for an individual The Grange Family Medical Centre must ensure that the individual is aware that we have collected this information and the circumstances of that collection, why we collect that information and the consequences for the patient if we don't collect it.

APP5 – NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION

Each new patient to the practice is asked to complete a Registration and Consent form, at which time they are also provided with a copy of our Practice Information sheet and advised that they can request to see a full Privacy Policy. All new patients are interviewed by the Practice Nurse for their family and social histories; weight and blood pressure to be entered into the patient file. In the Practice Nurse's absence, patient are asked to complete an Update Your Details Form instead, and are asked to hand this to their GP who will update their records. Your GP will also ask further personal health information to complete a picture of your current and past health information.

An Update Your Details Form is held at the front counter for patients to update any demographic details. Other information such as family or social history should be updated with your GP at your consultation.

To enable us to obtain copies of other personal information that we require, we will on an as needs basis ask for your consent, either verbally if the patient is not present in the practice, or by signing our consent form, prior to soliciting the information we require. All actions to this effect are documented in your file.

APP6 – USE OR DISCLOSURE OF PERSONAL INFORMATION

- Information regarding individual patients will not be disclosed in any form except for strictly authorised use for patient care or as legally directed. Failure to abide by this directive will result in disciplinary action, possible dismissal and other legal consequences. Each staff member must sign a confidentiality agreement.
- In our practice, items for pathology couriers and other pick-ups are left behind the reception desk.
- For primary purpose and related secondary purpose your personal health information can only be accessed via authorised GPs and staff. Staff who access files have signed privacy agreements. The Practice Manager and reception staff and nurses require access to accounts, demographic records and from time to time actual medical records. GPs are also aware of privacy restrictions and access issues and use passwords for computer access.
- Patients referred to another health service provider will be aware that their personal health information will be included in their referral letter/request, given to that service provider for the normal course of ongoing patient care and management. The patient has the right to not to give consent to this, however they would then not be referred to that provider! Pathology/Radiology, other medical, dental specialists, and allied health care service providers included here. These referrals are handed to the patient, and where deemed necessary are also faxed, or emailed in an encrypted format to the relevant service provided.

There are instances where patient information is requested by another health service provider, such as the Emergency Department of a Hospital – where the patient is being seen and they request a copy of the patient's health summary. We provide this to them to assist in patient care and management, and document this action in your file.

Where patients have been presented with a referral to another health service provider, then present for their appointment without the associated referral, we will at the request of either the patient or that health service provider forward a copy of the initial referral. Documenting the action taken in the patient file.

For other requests/disclose of information we will either telephone you and ask for your consent, telling you what we have been asked to release, to whom and why. If you are in the practice at the time, we will ask you to sign a consent form, advising what has been requested, by whom and why.

- Account details only provided to gain payment from insurance/Medicare office.
- No additional unnecessary data given
- Under certain legislation we must disclose patient information eg Infectious Diseases Act – Health (Infectious Diseases) Regulations, Adoption Act. Records must be disclosed under court orders, subpoenas, search warrants and Coroner’s Court cases.
- Visiting Medical Students, with patient consent, may access patient file to present patient case history to teaching GP. All Medical Students sign confidentiality agreements
- All contactors retained by Focus Medical Centre also sign confidentiality agreements.

APP7 – DIRECT MARKETING

We do not release your information to direct marketing companies and do not participate in direct marketing.

APP8 – CROSS-BORDER DISCLOSURE OF PERSONAL INFORMATION

We do not disclose personal information to overseas recipients

APP9 – ADOPTION, USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

We do not adopt, use or disclose government related identifiers of an individual unless permitted by an Australian law or court/tribunal order.

APP10 – QUALITY OF PERSONAL INFORMATION

We endeavour to ensure that the personal information that we collect is accurate, up-to-date and complete. An Update Your Details Form is available at the front counter for patients to update personal information.

APP11 – SECURITY OF PERSONAL INFORMATION

In our practice, to ensure the maintenance of privacy and security, health records are stored on the computer. Computer screens are positioned so that individuals cannot see information about other individuals. Access to computerised patient information is strictly controlled with passwords and personal logins, automatic screen savers and computer terminals are logged off when the computer is left unattended for a significant period of time so that unauthorised persons are unable to access information.

APP12 – ACCESS TO PERSONAL INFORMATION

- Patients of our practice have the right to access their own personal health information under the Federal Privacy Act 1998 and the APP (Australian Privacy Principles), with noted exceptions.
- On receipt of a written request for access to personal health information, our practice documents each request and endeavours to assist patients in granting access where possible and according to the privacy legislation. This correspondence should be addressed to Dr Debra King, GP or Lauren Schneider, Practice Manager; The Grange Family Medical Centre, Suite 1/82 Lake Road, Port Macquarie NSW 2444. Phone: 6584 5244 to discuss further.
- We forward the patient request to the patient’s GP to check for exemptions. Exemptions to access must be noted and each patient or legally nominated representative must have their identification checked prior to access being granted.
- The request and approval must be scanned into the record.

- As a patient must not have unsupervised access to the computer, a staff member must be present at all times to access the documents for the patient, when required. Both active and inactive patient health records are kept and stored securely. A fee may be charged.
- If a patient feels that the information in their file is incorrect, this matter will be dealt with on a case-by-case situation. The patient would be requested to provide in writing reasoning as to what information needs to be corrected and evidence as to why. Then an appointment would be made for the GP to discuss this matter with the patient.

Situations in which health records may need to be transferred from our Practice include:

1. A patient requests records to be sent to another practice
2. Legal reasons eg subpoena
3. Where health records are requested from another source

The particular GP is to be notified. The request is to be scanned into the patient's file and must include all details. The written request must be signed by the patient. All records are retained in the computer records, and only a copy will be sent. The Practice retains the right to charge a fee for the transfer of records. Practices are advised to contact their insurers if they have any concerns about third party request for transfer of patient health information.

APP13 - CORRECTION OF PERSONAL INFORMATION

We take reasonable steps to correct personal information to ensure that our information is accurate, up-to-date, complete, relevant and not misleading.

COMPLAINTS

Our Policy is to treat all Complaints seriously, to acknowledge receipt of complaint, maintain a register of complaints and resultant actions, discuss issues within the complaint and solve the problem if we are able. If no resolution can be made, details of appropriate tribunals for the complainant to contact will be given to the complainant to take the issue further.

DATA BREACH

Should the practice become aware of a data breach, we will notify the individual whose personal information has been breached. This will provide a reasonable step in the protection of this information against misuse, loss or unauthorised access.

As a practice we will explain what has gone wrong and what has been done to try to avoid a repeat situation, as well as what has been done to remedy any potential harm. We will help patients regain control of information eg, change passwords and request re-issue of identifiers.

We will endeavour to regain public trust. We take the protection of your personal information seriously. Our data breach response includes notifying the patient. Serious breaches will involve notifying the OAIC and and relevant 3rd parties.

If a patient believes there has been a breach of the Australian Privacy Principles (APP) in the first instance they should make the practice aware. If the patient is not satisfied with the Practice response they can lodge a complaint with the OAIC (Office of the Australian Information Commissioner).

Phone: 1300 363 992
Facsimile: 9384 9666

GPO Box 5218
SYDNEY NSW 2001

HOW LONG IS YOUR PERSONAL HEALTH INFORMATION KEPT

Our practice refers to State or Territory and/or Federal legislation regarding the length of time patient health records must be kept. This includes those that are inactive and when the patient is deceased. Our practice also consults our medical defence organisation regarding requirements.

At a minimum, patient health records must be kept until the patient is 25 years of age, if a child, or a minimum of 7 years following the last year of the patient's attendance, whichever is greater. Patient account records must be retained for a minimum of 7 years.

RESEARCH

The Practice does not involve itself widely in research and quality programs due to our strong belief in patient confidentiality. There will be odd occasions when it is felt appropriate to vary that stance.

Wherever possible, patient data should be de-identified, however if it is unavoidable, our practice ensures:

- The patient provides explicitly and documented written consent
- The patient received a written and verbal explanation about the research
- The patient can withdraw their consent at any time
- The project is approved by a relevant Human Research Ethics Committee (HREC) established under the National Health and Medical Research Council guidelines
- Privacy laws are followed.

WHO IS RESPONSIBLE FOR THIS

Our practice has a designated person (Dr Adam King) 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 5.1). 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 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 electronic 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 assessed by appropriate team members when required. We also ensure information held about the patient in different records (eg, at a residential aged care facility) is available when required