C6.3A Practice privacy policy

Introduction

This privacy policy is to provide information to you, our patient, on how your personal information (which includes your health information) is collected and used within our practice, and the circumstances in which we may share it with third parties. The practice will require sufficient information to identify the patient and document their care, including reasons for visits, management, progress and outcomes.

Why and when your consent is necessary.

When you register as a patient of our practice, you provide consent for our GPs and practice staff to access and use your personal information so they can provide you with the best possible healthcare. Only staff who need to see your personal information will have access to it. If we need to use your information for anything else, we will seek additional consent from you to do this.

Why do we collect, use, hold, and share your personal information?

Our practice will need to collect your personal information to provide healthcare services to you. Our main purpose for collecting, using, holding, and sharing your personal information is to manage your health. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (eg staff training).

What personal information do we collect?

The information we will collect about you includes your:

- names, date of birth, addresses, contact details
- medical information including medical history, medications, allergies, adverse events, immunisations, medical and social history, family history, and risk factors.
- Medicare number (where available) for identification and claiming purposes.
- healthcare identifiers
- Investigation requests and results
- Preventive care and health summaries
- Diagnosis and management plans

Various types of images may be collected and used, including

- CCTV Footage – Collected on our premises for safety and security.
- Photos and Medical Images: These can be taken using personal devices for medical purposes, following the guidelines.

Dealing with us anonymously

You have the right to deal with us anonymously or under a pseudonym unless it is impracticable for us to do so or unless we are required or authorised by law to only deal with identified individuals.

How do we collect your personal information?

Our practice may collect your personal information in several different ways.

1. When you make your first appointment our practice staff will collect your personal and demographic information via your registration.
2. During the course of providing medical services, we may collect further personal information. Information can also be collected through electronic transfer of prescriptions (eTP), My Health Record, eg via Shared Health Summary, Event Summary. You will need to specify if your practice participates in any of these eHealth services.
3. We may also collect your personal information when you send us an email or SMS, telephone us, make an online appointment or communicate with us using social media.
4. In some circumstances personal information may also be collected from other sources. Often this is because it is not practical or reasonable to collect it from you directly. This may include information from:
    - your guardian or responsible person
    - other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services, and pathology and diagnostic imaging services
    - your health fund, Medicare, or the Department of Veterans Affairs (as necessary).

When, why, and with whom do we share your personal information?

We sometimes share your personal information:

- with third parties who work with our practice for business purposes, such as accreditation agencies information technology providers – these third parties are required to comply with APPs and this policy.
- with other healthcare providers
- when it is required or authorised by law (eg court subpoenas)
- when it is necessary to lessen or prevent a serious threat to a patient's life, health or safety or public health or safety, or it is impractical to obtain the patient's consent.
- to assist in locating a missing person
- to establish, exercise or defend an equitable claim.
- for the purpose of confidential dispute resolution process
- when there is a statutory requirement to share certain personal information (eg some diseases require mandatory notification)
- during the course of providing medical services, through eTP, My Health Record (eg via Shared Health Summary, Event Summary).

How are document technologies used?

Document automation is where systems use existing data to generate electronic documents relating to medical conditions and healthcare.

The practice uses document automation technologies to create documents such as referrals, which are sent to other healthcare providers. These documents contain only your relevant medical information.

These document automation technologies are used through secure medical software Medical Director.

All users of the medical software have their own unique user credentials and password and can only access information that is relevant to their role in the practice team.

The practice complies with the Australian privacy legislation and APPs to protect your information. All data, both electronic and paper are stored and managed in accordance with the Royal Australian College of General Practitioners

Our Practice conducts Telehealth Consultations as well as face-to-face consultations. Reasonable steps are taken to protect the privacy and confidentiality of patients. The consultation is only conducted following consent from the patient. As we bulk bill, the patient will receive a bulk bill consent form to return to the Doctor so Medicare can get billed.

Only people who need to access your information will be able to do so. Other than in the course of providing medical services or as otherwise described in this policy, our practice will not share personal information with any third party without your consent.
We will not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

Our practice will not use your personal information for marketing any of our goods or services directly to you without your express consent. If you do consent, you may opt out of direct marketing at any time by notifying our practice in writing.

Our practice may use your personal information to improve the quality of the services we offer to our patients through research and analysis of our patient data.

We may provide de-identified data to other organisations to improve population health outcomes. The information is secure, patients cannot be identified, and the information is stored within Australia. You can let our reception staff know if you do not want your information included.

How do we store and protect your personal information?

Your personal information are stored at our practice in our Best Practice software.

All records after being scanned are sent to a facility for confidential destruction. All x-rays stored are required to be picked up by patients, if not picked up within 3 months of arrival to the practice theses will be sent for confidential destruction.

Our practice stores all electronic medical records on site electronically and are password protected.

How can you access and correct your personal information at our practice?

You have the right to request access to, and correction of, your personal information.

Our practice acknowledges patients may request access to their medical records. We require you to put this request in writing via a form available at reception and our practice will respond within a 14 day period. For a full record of your file there is a fee of $60.00 for associated time and printing costs.

Our practice will take reasonable steps to correct your personal information where the information is not accurate or up to date. From time to time, we will ask you to verify that your personal information held by our practice is correct and current. You may also request that we correct or update your information at reception when you come in for an appointment, or if medical with your GP or a practice nurse.

How can you lodge a privacy-related complaint, and how will the complaint be handled at our practice?

We take complaints and concerns regarding privacy seriously. You should express any privacy concerns you may have in writing. We will then attempt to resolve it in accordance with our resolution procedure. Our practice manager, Wendy Evans handles all complaints and a form will be provided if asked. Wendy Evans can be contacted on 8258 9103 and her email is pm@europamedical.com.au if you wish to email. This will be taken into consideration and confirmation will be provided and handling will be processed in due course within 30 days.

You may also contact the ***Office of the Australian Information Commissioner*** (***OAIC***). Generally, the OAIC will require you to give them time to respond before they investigate. For further information visit www.oaic.gov.au or call the OAIC on 1300 363 992.

Privacy and our website

Our practice website does not collect personal information of our patients,

Policy review statement

This privacy policy will be reviewed regularly to ensure it is in accordance with any changes that may occur. State how you will notify your patients when you amend this policy.

Disclaimer

The *Privacy policy template for general practices* is intended for use as a guide of a general nature only and may or may not be relevant to practices or circumstances. The Royal Australian College of General Practitioners (RACGP) has used its best endeavours to ensure the template is adapted for general practice to address current and anticipated future privacy requirements. Persons adopting or implementing its procedures or recommendations should exercise their own independent skill or judgement or seek appropriate professional advice. While the template is directed to general practice, it does not ensure compliance with any privacy laws, and cannot of itself guarantee discharge of the duty of care owed to patients. Accordingly, the RACGP disclaims all liability (including negligence) to any users of the information contained in this template for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of reliance on the template in any manner.

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 consent has been sought from the patient.

Reviewed 22nd February 2026

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

1.1.1. Procedure

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

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

As a rule, no patient information is to be released to a third 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 to the third party.

Written requests for the transfer of health information are noted in the patient's health record and are also documented in the practice's *Transfer Request* register. Any request received is forwarded to the patient's usual general practitioner for action. The requested record is to be reviewed by the general practitioner whilst using the *Release of Health Information Checklist* prior to release to a third party to ascertain if the information being requested is suitable for release.

To meet the costs associated with reviewing and preparing personal patient health information to be released to a third party, our practice does not charge a fee for the medical records.

Where patient information is being transferred in hard copy (i.e. post or being collected by the patient/third party), only copies are provided; the original is to remain at the practice.

The security of any health information requested is maintained when transferring requested records. Electronic data transmission of personal patient health information from our practice is in a secure format.

Subpoena, court order, coroner search warrant
Where a request for patient information is being sought by subpoena, court order, or coroner search warrant, we note the date of the pending court case and the date the request was received in the patient's health record. Depending on whether a physical or electronic copy of the record is required, we follow the procedures as described above.

On occasions, a member of the practice team is required to accompany the patient's health record to court or, alternatively, a secure courier service may be adequate. If the original is to be transported, we ensure a copy is made in case of loss of the original document during transport and we ensure that the record is returned after review by the court (refer to **Section 8 – Management of potential medical defence claims**).

Relatives/friends
A patient may authorise another person to be given access to their health information if they have the legal right and a signed authority (refer to **Section 6.5 – Request for access to personal health information**).

If a situation arises where a career is seeking access to a patient's health information, we contact our medical defence organisation for advice before such access is granted.

Significant court orders relating to custody and guardianship are recorded as an alert on the health records of children where appropriate to ensure no information is released to an unauthorised party.

External practitioners and healthcare institutions
Any requests received from general practitioners or other healthcare institutions, external to our practice, are directed to the patient's usual general practitioner, or to the Practice Manager.

Police/solicitors
All members of the practice team have been made aware of the requirement for police and solicitors to obtain case-specific signed patient consent (or subpoena, court order or search warrant) before any information relating to that patient is released. Any such requests received are directed to the patient's usual general practitioner.

Health insurance companies/workers compensation/social welfare agencies
Depending on the specific circumstances, information may need to be provided and any such requests received are referred to the patient's usual general practitioner.

Employers
If the patient has signed consent to release information for a pre-employment questionnaire or similar report, this request is referred to the patient's usual general practitioner.

Government agencies – Medicare/Department of Veterans Affairs
Depending on the specific circumstances, information may need to be provided and any such requests received are referred to the patient's usual general practitioner with a recommendation to discuss any issues with their medical defence organisation.

State registers of births, deaths, and marriages
Death certificates are to be issued by the patient's usual general practitioner.

Accounts/debt collection
The practice must maintain privacy of a patient's financial accounts.

Accounts must not contain any clinical information. Invoices and statements are reviewed prior to forwarding to third parties, such as insurance companies or debt collection agencies.

Outstanding account queries or disputes are directed to the Practice Manager.

Students (medical and nursing)
Our practice participates in medical student education. We acknowledge that some patients may not wish to have their personal health information accessed for educational purposes; therefore, the practice always advises patients of impending student involvement in practice activities and seeks to obtain patient consent accordingly.

Research and continuous quality improvement activities
Where our practice seeks to participate in human research activities and/or continuous quality improvement activities, patient confidentiality and privacy will be maintained. Only the information of patients who have provided their explicit consent for the practice to use their information for these activities in this manner will be used. A copy of the patient consent to any specific data collection for research or continuous quality improvement purposes is retained in their record.

All requests to participate in research are to be approved by the practice principal/practice owners before commencing, and also must have approval from a Human Research Ethics Committee (HREC) constituted under the NHMRC guidelines. A copy of this approval is retained by the practice. Also refer to **Section 7.11 – Resource projects**.

Media
No member of the practice team is permitted to release information to media outlets unless it has been authorised, and all enquiries are to be directed to the Practice Manager.

International
Where patients request and consent to have their information transferred overseas, this can be performed; however, where the request for transfer of information is received by international subpoena, our practice is under no obligation to comply.

Disease registers
This practice submits patient data to various diseases registers to assist with preventative health management (e.g. cervical, breast and bowel screening, etc.).

Consent is required and obtained from the patient to 'opt in' to have their information shared with these registers. This consent is obtained when the patient first attends the practice, and patients are reminded through signage in the waiting room and by information contained in the practice information sheet of the opportunity to revisit their previous consent/non-consent to this data sharing at any time.