

Privacy Policy

Last updated: September 2025

The objective of this privacy notice is to provide you, our patient, with clear information on how your personal information is collected and used within the practice. Occasionally we also need to share your personal information to involve others in your healthcare and this policy outlines when, how, and why we share your information.

For enquiries concerning this policy, you can contact: hello@yourhealthgp.com.au

1. When and why is your consent necessary?

When you register as a patient of this practice, you provide consent for the GPs and practice staff to access and use your personal information to facilitate the delivery of healthcare. Access to your personal information is restricted to practice team members who require it for your care. If we ever use your personal information for purposes other than healthcare provision, we will obtain additional consent from you.

It is important to us that as our patient, you understand why we collect and use your personal information.

2. Why do we collect, use, store, and share your personal information?

The practice collects, uses, stores, and shares your personal information primarily to manage your health safely and effectively. This includes providing healthcare services, managing medical records, and ensuring accurate billing and payments. Additionally, we may utilise your information for internal quality and safety improvement processes such as practice audits, accreditation purposes, and staff training to maintain high-quality service standards.

3. What personal information is collected?

The information we will collect about you includes your:

- names, date of birth, addresses, contact details and next of kin and emergency contact
- medical information including medical history, medicines, allergies and adverse reactions, immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- healthcare identifier numbers
- concession card and DVA number if applicable

4. Can you deal with us anonymously?

You can 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.

5. How is personal information collected?

The practice may collect your personal information in several different ways:

- When you make your first appointment, the practice team will collect your personal and demographic information via your registration.
- We may also collect your personal information when you visit our website, send us an email or SMS, telephone us, make an online appointment, or communicate with us using social media.

In some circumstances, personal information may also be collected from other sources, including:

- 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 (if relevant).

While providing medical services, further personal information may be collected via:

- electronic prescribing
- My Health Record
- online appointments.

Photos and medical images: These can be taken using personal devices for medical purposes, following the guidelines outlined in our guide on using personal devices for medical images.

We will always comply with privacy obligations when collecting personal information from third-party sources. This includes ensuring transparency with patients, obtaining necessary consents, maintaining data accuracy, securing the information, and using it only for specified purposes.

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

We sometimes share your personal information:

- with third parties for business purposes, such as accreditation agencies or information technology providers – these third parties are required to comply with APPs and this policy
- with other healthcare providers (e.g. in referral letters)
- when it is required or authorised by law (e.g. 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 it is a statutory requirement to share certain personal information (e.g. some diseases require mandatory notification)
- when it is provision of medical services, through electronic prescribing, My Health Record (e.g. via Shared Health Summary, Event Summary).

Only people who need to access your personal information will be able to do so. Other than providing medical services or as otherwise described in this policy, the practice will not share personal information with any third party without your consent.

We do not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

We transmit referrals via HealthLinks (a secure messaging system with end-to-end encryption), email and/or fax. Our preference is to send referrals via HealthLinks but some specialists and many allied health do not have

access to Healthlinks and so in these situations we use email. Note that our emails do not have end-to-end encryption. We will ask your verbal permission to send referrals via email.

7. Our practice uses HotDocs and HealthEngine for appointment bookings and confirmation

Our practice uses HotDocs and HealthEngine to facilitate booking appointments. We also use HotDocs to send appointment reminders via SMS. These third party integrations have access to the bare minimum of information required to facilitate appointment bookings and appointment reminders, which will generally include the patient's name, date of birth, contact details, Medicare information, and appointment information (e.g. time, date, appointment type, and practitioner name).

These third party integrations do not have access to patients' medical records, or anything discussed with their doctor in their appointment. HotDocs and HealthEngine comply with the Australian Privacy Act, and information stored by these third party integrations are stored in Australia. You will receive SMS reminders for your appointment, from HotDoc, even if you do not book an appointment via their service, as we have signed an agreement with them to manage our appointment reminders via SMS. If you would like to opt-out of SMS reminders from HotDocs please let us know so we can action your request.

8. How does the practice use SMS and email?

When you become a patient of our practice you are asked to provide your consent to be sent communications via SMS and email, or alternatively you may select to opt-out of these forms of communication. Our email is encrypted but not end-to-end encrypted, and by sending and receiving emails to us you consent to accepting risks of sending personal information via email. Our practice deletes emails containing specialist letters and transferred medical records once they have been imported into your medical records in our practice management software. For further information regarding how our practice communicates with patients, please refer to our Communications Policy.

9. Will your information be used for marketing purposes?

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

10. How is your information used to improve services?

The practice may use your personal information to improve the quality of the services offered to patients through research, analysis of patient data for quality improvement and for training activities with the practice team

Our practice shares de-identified data with Capital Health Network to support quality improvement and better patient-centred care. This is done through POLAR (Population Level Analysis and Reporting), a secure, cloud-based clinical intelligence tool developed by Outcome Health for general practices. POLAR automatically extracts de-identified data, that is encrypted using secure, industry-standard methods (similar to banking systems) and uploads that data to a secure national POLAR warehouse. The purpose of this process is to help improve primary healthcare in our region and assess community health needs. If you would like to opt-out of your deidentified data being shared with POLAR please let us know so we can action your request.

11. How are document automation 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 Best Practice.

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 [Privacy and managing health information guidance](#).

12. How is your personal information stored and protected?

The practice stores information in electronic records and photos stored in your electronic file.

Our staff are trained and required to respect and protect your privacy. We take reasonable steps to protect information held from misuse and loss and from unauthorised access, modification or disclosure. This includes:

- Utilising strong password protections
- Electronic information is held in secure cloud storage
- Our staff sign confidentiality agreements
- Our practice has document retention and destruction policies

Data is stored and managed by our IT provider GP Support in their secure Equinix facility in Port Melbourne, and data is backed up regularly according to our Data Recovery Plan.

13. How long is my data stored for?

Your electronic records are stored in our practice management software for a minimum of 7 years from the date of the provision of the last health service, or until a young person turns 25 years. This is in accordance with ACT legislation.

Paper records such as paper forms and medical correspondence are disposed of securely by a cross-cut shredder or medical records confidential waste service after becoming digitised and are not stored at our medical practice.

14. How can you access and correct your personal information at the practice?

You have the right to request access to, and correction of, your personal information. You may request we correct or update your information via email at hello@yourhealthgp.com.au

We will normally respond to your request within 30 days.

The practice will take reasonable steps to correct your personal information where the information is not accurate or up to date. Sometimes, we will ask you to verify your personal information held by the practice is correct and current.

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

We take complaints and concerns regarding privacy seriously. You should express any privacy concerns you may have. We will then attempt to resolve it in accordance with the resolution procedure.

If you would like to make a complaint, please email us at hello@yourhealthgp.com.au . Alternatively you can mail us at Erindale Chambers, 4/5 Grattan Court, Wanniasa ACT 2903 or call us at 02 5138 1606. We will aim to respond to your complaint within 30 business days.

If you do not feel we have resolved your issue you may also contact the Office of the Australian Information Commissioner. The Office of the Australian Information Commissioner will require you to give them time to respond before they investigate. For further information visit www.oaic.gov.au or call the OAIC (Office of the Australian Information Commissioner) on 1300 363 992.

16. How is privacy on the website maintained?

At Your Health General Practice, any personal information you share with us through website or email is handled securely and confidentially. This practice uses analytics and cookies.

Cookies are small pieces of data stored on a site visitor's browser. They are typically used to keep track of the settings users have selected and actions they have taken on a site. Our website is hosted by Wix, which uses cookies for reasons such as to monitor and analysis the performance, operation and effectiveness of our website, and to ensure that the website platform is secure and safe to use. Our website only uses essential cookies.

Our website uses analytics to monitor our website activity.

17. Policy review statement

Our privacy policy is regularly reviewed to ensure compliance with current obligations.

If any changes are made:

- They will be reflected on the website.
- Significant changes may be communicated directly to patients via email or other means.

Please check the policy periodically for updates. If you have any questions, feel free to contact us.