

Boyup Brook Medical Services Privacy Policy

Introduction

This privacy policy explains how our practice collects, uses and protects your personal information — including your health information — and the circumstances in which we may share it with third parties.

A 'patient health record' is the record we create and maintain about your care, including your clinical notes, test results, correspondence, referrals, and other health-related information we hold about you.

This policy is available on our practice website, and a printed copy is available free of charge from reception on request.

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 information will have access to it. If we need to use your information for anything else, we will seek additional consent from you. In some circumstances, the law may authorise us to collect, use or disclose your information without your consent — for example, to lessen or prevent a serious threat to life, health or safety, or where required by law.

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

Our practice collects your personal information to provide healthcare services to you. Our main purpose is to manage your health and wellbeing. We also use it for directly related activities, such as processing claims and payments, practice audits and accreditation, and business processes like staff training.

Is my personal information used for automated decision-making?

Yes. Under the Privacy and Responsible Information Sharing Act 2024 (WA), we use AI-powered medical scribes to assist with clinical documentation. These tools capture consultations and use AI to generate draft notes, referral letters and summaries. Our clinicians review, edit and approve all documentation before it becomes part of your record. Automated decision-making includes where a clinician's decision is materially assisted by an AI system. If an automated process involving your personal information is used to make a significant decision about you (affecting your rights, interests or circumstances), we will:

- Notify you that an automated process has been used
- On request, explain how the process works in plain language
- Provide a way for you to request human intervention

If you would like more information or wish to request human review of a decision, please contact us at reception@boyupmedical.com.au.

Where document automation technologies (including AI-generated drafts) are used to prepare referral letters or clinical summaries, our clinicians review each document before it is sent to ensure it is accurate and that only information relevant to the referral or communication is included.

What personal information do we collect?

The information we collect about you includes:

- Personal information — names, date of birth, addresses, contact details, Medicare number (where available), healthcare identifiers, and health fund details
- Sensitive information — medical information including your medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors

We only collect information that is directly related to providing you with healthcare services.

What are the consequences of not providing personal information?

Providing your personal information helps us deliver safe and effective care. If you choose not to provide some or all of the information we request, the following consequences may apply:

- We may be limited in our ability to accurately assess, diagnose or treat your condition
- We may not be able to refer you to specialists or arrange other healthcare services
- We may be unable to process Medicare claims, health insurance rebates or other billing on your behalf
- The quality and completeness of your clinical records may be affected, which could impact continuity of care
- In some cases, we may need to decline to provide a particular service if we do not have sufficient information to do so safely

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.

For example, it may be impracticable for us to deal with you anonymously when providing direct medical care, processing Medicare claims, notifying a reportable disease, or investigating a complaint. In these situations, we will need to collect your name and other identifying information.

How do we collect your personal information?

Our practice will collect your personal information:

- When you make your first appointment, our practice staff will collect your personal and demographic information via your registration
- During the course of providing medical services, we may collect further personal information — including through Electronic Transfer of Prescriptions (eTP) and the My Health Record system
- When you send us an email, SMS or telephone us
- From other sources where 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, and pathology services), your health fund, Medicare, or the Department of Veteran's Affairs

Who do we share your personal information with?

We sometimes share your personal information:

- with third parties who work with our practice 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

- when it is required or authorised by law (e.g. court subpoenas)
- when it is necessary to lessen or prevent a serious threat to life, health or safety of an individual or the public or it is impractical to obtain the patient's consent
- a reasonable belief exists that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of another individual who is a genetic relative of the first individual
- 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 (e.g. some diseases require mandatory notification)
- during the course of providing medical services, through Electronic Transfer of Prescriptions (eTP), MyHealth Record/PCEHR system (e.g. via Shared Health Summary, Event Summary)

Only people that 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.

When we share or transfer your personal information — including with other healthcare providers, government agencies, or other parties described in this policy — we use secure electronic communication methods or other appropriate safeguards, such as encryption or secure messaging systems, to protect your information during transfer.

How do we store and protect your personal information?

Your personal information is stored at our practice as electronic records. We take reasonable steps to protect your information from misuse, loss, unauthorised access, modification or disclosure.

Our security measures include:

- Physical security at our practice premises
- Electronic security systems, including access controls and encryption where appropriate
- System back-up procedures to safeguard against data loss
- Secure storage of prescription pads, letterhead, and other official practice documents, accessible only to authorised staff

Your personal information may be held by third-party data storage providers engaged by us. We require all third parties who handle your information to comply with applicable privacy laws.

Records retention and destruction

We retain your personal information in accordance with the State Records Act 2000 and other mandatory requirements that are or may come into effect such as the General Retention and Disposal Authority for Local Government Information. When information is no longer required, we take reasonable steps to destroy or de-identify it securely and in compliance with legal obligations.

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 held by us.

If you'd like to access or correct your information, simply put your request in writing. You can do this by completing and signing our request form, available at reception, or by sending a written request to our Practice Manager at practicemanager@boyupmedical.com.au or by post to 78b Abel St, Boyup Brook WA 6244. Just make sure your request includes enough detail for us to identify the relevant documents and provide an address in Australia for our response.

Your request will be handled under the Freedom of Information Act 1992 (WA). We'll respond within the timeframes set out in that Act — up to 45 days for access requests and 30 days for correction requests. Importantly, no fee is charged for providing you with access to your own personal information. Where possible, we prefer to send information by secure email.

If you believe the information we hold is inaccurate, incomplete, out of date or misleading, please let us know in writing with details of the information and the correction you're seeking. If we decide not to make the amendment, you can request that a notation be added to your record explaining your concerns.

In limited circumstances, we may need to refuse access — for example, if disclosure could adversely affect your health, reveal another person's information without their consent, or prejudice a law enforcement investigation. If this applies, we'll let you know. We'll also take reasonable steps to verify your identity before providing access, to make sure your information only goes to you or someone you've authorised in writing.

SMS, email and My Health Record

This practice may use SMS and email for appointment reminders, recalls and other reminders or medical services. Our practice may also upload Shared Health Summaries to My Health Record. If you do not consent to this, please advise our receptionist.

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

We take privacy complaints seriously. If you have a concern, please put it in writing to our Practice Manager at practicemanager@boyupmedical.com.au or by post to 78b Abel St, Boyup Brook WA 6244, and include your mailing address and contact number.

We will acknowledge your complaint and aim to resolve it within 30 days.

If you're not satisfied with the outcome, you may apply for an internal review under the Freedom of Information Act 1992 — your application must be in writing within 30 days of receiving our decision.

You may also take your complaint to an external body:

- Office of the Australian Information Commissioner — www.oaic.gov.au or 1300 363 992
- Health and Disability Services Complaints Office (HaDSCO) — 1800 813 583
- Information Commissioner (WA) — for complaints under the *Privacy and Responsible Information Sharing Act 2024*

RACGP Standards for General Practices (5th edition) – criteria addressed by this policy

This policy has been developed to address the following criteria and indicators of Core Standard 6 – Information management:

- **Criterion C6.3** – Confidentiality and privacy of health and other information
- **C6.3 A** – Our patients are informed of how our practice manages confidentiality and their personal health information.
- **C6.3 B** – Our patients are informed of how they can gain access to their health information we hold.
- **C6.3 C** – In response to valid requests, our practice transfers relevant patient health information in a timely, authorised, and secure manner.
- **C6.3 D** – Only authorised team members can access our patient health records, prescription pads, and other official documents.
- **Criterion C6.4** – Information security
- **C6.4 E** – Our practice has appropriate procedures for the storage, retention, and destruction of records.

Other indicators under Criterion C6.4 relating to IT and computer security responsibilities, system access controls, business continuity, and the use of email and social media are addressed in the Medical Centre's separate IT and Information Security Policy.

Policy review statement

This policy will be reviewed regularly to ensure it is in accordance with any changes that may occur.

Document Control		
Created: 2016		
Reviewed: Sept 2026	Reviewer: Sarah Alexander (Practice Manager)	Next Review: September 2027