PRIVACY STATEMENT

Banksia Medical & Health | Patient information | Version 2.0 | Prepared November 2026

Introduction

Banksia Medical & Health respects your privacy. This statement explains how we collect, use, store and disclose personal information, including sensitive health information, and how you may access or correct it. We handle information in accordance with applicable Australian privacy laws, including the Privacy Act 1988 and Australian Privacy Principles.

What information we collect

Depending on the care or service provided, we may collect your name, date of birth, contact and identification details, Medicare and other relevant payment details, medical history, medications, allergies, clinical notes, test results, referrals, appointment information and correspondence. We collect only information reasonably necessary for our functions and services.

How information is collected

Information may be collected directly from you, your authorised representative, treating clinicians, hospitals, pathology and imaging providers, other health services, and approved digital health systems, where lawful and appropriate. Where practical, we explain why information is needed and the consequences of not providing it.

Consent and use of information

We use your information primarily to provide and coordinate healthcare, manage appointments, communicate with you, maintain accurate health records, arrange referrals and investigations, and undertake billing and lawful practice administration. Other uses or disclosures will occur only where you consent or the law permits or requires them. Consent is sought when legally or clinically required; registration alone does not authorise every possible use or disclosure.

Access by practice staff

Only authorised staff and clinicians may access patient information as necessary for their duties. Access is subject to confidentiality obligations, role-appropriate permissions and practice security controls.

Disclosure to other parties

Where permitted, information may be shared with treating healthcare professionals, hospitals, pathology and imaging providers, Medicare and relevant funding bodies, authorised service providers supporting practice operations, and other recipients where you consent or disclosure is required or authorised by law. We verify identity and authority before releasing records to family members, employers, insurers or other third parties. Disclosures are limited to what is necessary and appropriate.

My Health Record and digital health

Where the practice participates in My Health Record, electronic prescribing, secure messaging or other digital health services, information is handled under the applicable laws, system rules and patient preferences. Ask our team how these services apply to your care and what choices are available.

Electronic communication

The practice may use telephone, SMS, email, online booking and secure messaging for suitable communications. Electronic channels can carry privacy risks. We take reasonable precautions, verify recipients and use secure channels for sensitive information where appropriate. Email and SMS are not suitable for urgent medical matters. Please advise us if you have communication preferences.

Anonymity and pseudonyms

You may request to interact anonymously or using a pseudonym where lawful and practicable. Identifying information is generally required to provide safe clinical care and meet health-record and billing obligations.

Storage and security

Patient information may be held in electronic and, where applicable, paper records. We take reasonable steps to protect information against misuse, interference, loss and unauthorised access, modification or disclosure. Safeguards may include restricted access, passwords, security controls, secure disposal and staff confidentiality requirements. Records are retained and disposed of in accordance with applicable legal obligations.

Access and correction

You may request access to or correction of personal information held about you. Contact the practice to make a request and verify your identity. Requests are considered under applicable privacy and health-record laws; access is not automatically dependent on a GP approving it. Reasonable fees may apply where legally permitted and will be explained in advance. If a correction cannot be made, you may ask for a statement of your requested correction to be associated with the record, where applicable.

Overseas disclosure

If information is likely to be disclosed to overseas recipients, the practice must identify the circumstances and relevant countries where practicable and meet applicable privacy requirements. **Practice confirmation required:** whether any current software, hosting, transcription or service arrangements involve overseas disclosure, and the relevant countries.

Privacy incidents and data breaches

Suspected privacy incidents should be reported promptly to the Practice Manager. The practice will assess, contain, document and respond to incidents, including assessing whether notification is required under the Notifiable Data Breaches scheme. A separate internal incident-response procedure governs staff actions.

Privacy complaints

Please raise privacy concerns with the Practice Manager, Banksia Medical & Health, at manager@banksiamedical.com.au. We will review the concern and respond through our complaints process. You may also contact the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au or 1300 363 992.

Website and online services

Information submitted through our website or online services may include contact details and information supplied in requests or forms. The collection and handling of this information should be explained at the point of collection where appropriate. Third-party online services may have their own privacy notices.

Availability and review

This statement will be made available to patients at the practice and through appropriate online channels. It will be reviewed at least annually and following significant changes to law, systems or practice operations.