Privacy Policy

Version 1.0 · Effective 15 September 2026

Rochedale Family Practice
1/734 Underwood Road, Rochedale South QLD 4123
(07) 3341 2022
reception@rochedalefp.com.au

Plain-language purpose

This policy explains how Rochedale Family Practice (RFP) collects, holds, uses, protects and discloses personal information, including health information, and how you can access or correct your information or raise a privacy concern.

1. Our privacy commitment

Rochedale Family Practice is committed to protecting the privacy and confidentiality of personal information. Health information is sensitive. We only collect and use information that is reasonably necessary for your care, safe practice operations and other lawful purposes.

This policy is intended to be read in plain language. It reflects the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), applicable digital-health laws and current guidance for private health service providers.

2. Why and when your consent is needed

When you register with RFP and receive care from us, you provide information so our doctors and authorised practice team members can provide healthcare and manage related services. We use or disclose your information for the purpose for which it was collected, for directly related purposes you would reasonably expect, or where otherwise permitted or required by law.

Where a proposed use or disclosure is outside those purposes, we will seek additional consent unless the law allows or requires us to act without consent.

3. What personal information we collect and hold

Depending on the services you use, we may collect and hold:

- identity and contact details, including name, date of birth, address, phone number, email and emergency-contact details
- health information, including medical history, symptoms, diagnoses, medications, allergies, adverse events, immunisations, investigation results, referrals, clinical notes, social and family history, risk factors and care plans
- Medicare details, Individual Healthcare Identifier and other healthcare identifiers where relevant
- Department of Veterans' Affairs, concession, private health insurance or other entitlement details where relevant
- appointment, recall, reminder, prescription, referral and communication records
- billing and payment information needed to process accounts, claims or refunds
- information supplied by a parent, guardian, substitute decision-maker or authorised representative
- clinical photographs, documents, audio or other recordings where clinically relevant and appropriately authorised

- technical information generated when you use our website or online services, such as IP address, browser/device information and security or server logs, where collected by the service.

4. How we collect your information

We usually collect information directly from you, including when you:

- register as a patient or update your details
- book or attend an appointment
- speak with us by phone or in person
- send an email, SMS or other approved message
- use our website, online forms, online booking or approved patient-request services
- provide documents, photographs, monitoring results or other health information.

We may also collect information from other sources when it is reasonable, necessary or not practical to obtain it directly from you. These sources may include:

- your parent, guardian, carer, substitute decision-maker or authorised representative
- other healthcare providers such as specialists, allied health practitioners, hospitals, pharmacies, pathology and diagnostic-imaging providers
- Medicare, the Department of Veterans' Affairs, private health insurers or other claim/payment bodies where relevant
- My Health Record and other authorised digital-health or secure clinical messaging systems.

5. Why we collect, use and disclose personal information

Our main purpose is to provide safe, continuous healthcare and manage your relationship with the practice. We may use or disclose information for:

- assessment, diagnosis, treatment, preventive care, follow-up and continuity of care

- referrals, prescriptions, investigations, care coordination and communication with other treating providers
- appointments, recalls, reminders, results follow-up and other patient communications
- Medicare, DVA, WorkCover, private billing, health-fund or other lawful claims and payments
- My Health Record and other authorised digital-health services
- practice accreditation, quality improvement, clinical audit, training and service evaluation, using the minimum information reasonably necessary
- responding to complaints, incidents, legal claims and professional or regulatory obligations
- public-health reporting, mandatory notifications, court orders or other uses/disclosures required or authorised by law
- lessening or preventing a serious threat to life, health or safety where the law permits disclosure without consent
- secure practice administration, fraud prevention, system security and business continuity.

6. Who we may share information with

We only disclose personal information when it is relevant and lawful. Recipients may include:

- other healthcare providers involved in your care
- pathology, diagnostic-imaging, pharmacy and allied-health services
- Medicare, DVA, WorkCover, private health insurers or other authorised claim/payment bodies
- My Health Record and authorised digital-health services
- approved service providers that support practice operations, such as information technology, secure messaging, online booking, SMS, software, cloud, payment, printing or accreditation providers, subject to appropriate privacy and confidentiality arrangements

- government, regulatory, law-enforcement, courts or other bodies where disclosure is required or authorised by law.

RFP does not sell patient personal information.

7. AI-assisted documentation and automated decisions

RFP clinicians may use approved AI-assisted clinical documentation tools, including Lyrebird, Heidi and MBS Pro, to assist with preparation of draft clinical notes and related documentation. These tools support documentation only; they do not replace clinical judgement or make autonomous decisions about patient care. The treating clinician reviews, edits where necessary and remains responsible for the final medical record.

Where an approved AI documentation tool needs to listen to, transcribe or record a consultation, the patient will be informed and consent will be sought before use, as required.

8. Overseas disclosure and cloud services

RFP uses external technology providers to support care and practice operations. Based on current practice, RFP does not disclose identifiable patient information to overseas recipients. If our systems or service arrangements change so that identifiable personal information is likely to be disclosed outside Australia, this policy will be updated and the relevant countries will be identified where practicable.

9. De-identified information, quality improvement and research

RFP may use or provide de-identified or aggregated information for quality improvement, service evaluation and population-health activities. Patients are not identified in this information. You may ask reception about opting out of routine de-identified data extraction where an opt-out is available. Where information is used or disclosed for research or another secondary purpose, RFP will comply with applicable privacy requirements, including consent or other lawful authority where required.

10. My Health Record and digital health

RFP participates in authorised digital-health services, including My Health Record where applicable. Information may be viewed, uploaded or shared through these systems in accordance with current legislation, system rules, access controls and your available My Health Record privacy settings.

11. Anonymity and pseudonyms

You may ask to deal with us anonymously or under a pseudonym where this is lawful and practical. In many clinical situations we need accurate identifying information to provide safe care, match results, prescribe, make Medicare claims or meet legal requirements. We will explain when identification is necessary.

12. How we protect and retain information

Personal information may be held in electronic clinical and business systems, secure communications, paper records and other authorised formats. RFP uses administrative, technical and physical safeguards appropriate to the sensitivity of health information.

- access is limited to authorised people who need information for their role
- users have authorised accounts and practice systems use access controls, screen locking and security protections
- approved secure clinical messaging is preferred for clinical information
- staff and contractors are bound by confidentiality and privacy obligations
- systems, backups and service providers are managed under RFP’s Information Security & IT Continuity Policy
- information is retained only for as long as required for clinical, legal, professional or operational purposes and is securely destroyed or de-identified when it is no longer required and lawful to do so.

CCTV operates in selected public and common areas of the practice for safety and security. CCTV records video only and does not record audio. Footage is accessed only by authorised persons and is retained or disclosed only where reasonably necessary or required or authorised by law.

If a suspected data breach occurs, RFP assesses and responds to it promptly. Where a breach is an eligible data breach under the Notifiable Data Breaches scheme, affected individuals and the Office of the Australian Information Commissioner (OAIC) will be notified as required.

13. Accessing your personal information

You may request access to personal information we hold about you. We may ask you to verify your identity and clarify what information you want and how you would like to receive it.

We aim to respond within a reasonable period, generally within 30 calendar days. In some circumstances the law allows access to be refused or limited; if this happens, we will explain the reason and available complaint options where required.

There is no fee to make an access request. A reasonable, non-excessive fee may apply to the cost of providing access. We will discuss any likely fee with you before access is provided.

14. Correcting your information

Please tell us if your personal information is incorrect, incomplete or out of date. We will take reasonable steps to correct it where appropriate. We aim to respond to a correction request within 30 calendar days.

There is no fee to request or make a correction. If we do not agree to a requested correction, we will explain the reason and your available options, including asking us to associate a statement with the record.

15. Privacy questions and complaints

We take privacy concerns seriously. Please contact our Privacy Officer so we can review the concern and try to resolve it promptly.

Privacy Officer

Jessica Ting, Operations & Business Manager

Email

reception@rochedalefp.com.au

(mark: Attention Privacy Officer)

Phone

(07) 3341 2022

Address

Rochedale Family Practice, Rochedale Health, 1/734 Underwood Road, Rochedale South QLD 4123

If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner (OAIC). You may also contact the Queensland Office of the Health Ombudsman about concerns relating to a health service.

16. Website, email and electronic communications

When you use our website, online forms or other electronic services, information may be transmitted through approved service providers. Please do not use routine email or website forms for urgent medical matters.

Electronic communications carry some inherent privacy and security risk. RFP uses reasonable safeguards and the minimum necessary information, and verifies recipients before sending sensitive information. You can ask us about alternative communication methods where appropriate.

17. Direct marketing

RFP does not use health information for direct marketing without consent or other lawful authority. If you consent to direct marketing, you may withdraw that consent or opt out at any time.

18. Policy availability and review

This policy is available free of charge on the RFP website and from reception on request. We review it at least annually and earlier if our information-handling practices, technology providers or legal obligations materially change.

When a material update affects how we handle personal information, we will take reasonable steps to make the updated policy known to patients, for example through our website, signage, forms or other appropriate communications.

19. References

- Privacy Act 1988 (Cth) and Australian Privacy Principles
- Office of the Australian Information Commissioner (OAIC), Guide to Health Privacy and APP Guidelines
- Notifiable Data Breaches scheme under the Privacy Act
- My Health Records Act 2012 (Cth) and current My Health Record Rules
- Healthcare Identifiers Act 2010 (Cth), where applicable
- RACGP Privacy policy template and current privacy/health-information guidance for general practice
- Rochedale Family Practice Information Security & IT Continuity Policy (2026).