



Introduction

Rotem Medical Pty Ltd ATF the Rotem Medical Family Trust (ABN 94 191 325 741) is committed to protecting the privacy of patient information and to handling your personal information in a responsible manner in accordance with the Privacy Act 1988, the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the Australian Privacy Principles (APPs) and relevant State and Territory privacy legislation (referred to as privacy legislation). 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. For enquiries concerning this policy, you can contact our Practice Manager – Natalie Ferris – on manager@rotemmedical.com.au

Why and when your consent is necessary?

When you register as a patient of a practitioner consulting at Rotem Medical Family 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. It is important to us that as our patient, you understand why we collect and use your personal information.

By acknowledging this Privacy Policy you consent to us collecting, holding, using, retaining and disclosing your personal information in the manners described below.

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

Our main purpose for collecting, using, holding, and sharing your personal information is to provide you with a premium healthcare service and inform you about the healthcare services offered at Rotem Medical Family Practice. We also use personal information for activities directly related to the supply of healthcare services, such as Medicare claims, payments, online booking, clinic audits, accreditation, staff training and to maintain high-quality service standards. We also communicate with patients using secure SMS notifications. If you receive healthcare from practitioners consulting from Rotem Medical Family Practice it is a requirement that you consent to be contacted by SMS regarding your appointments, outstanding accounts and healthcare information such as results notifications.

What personal information do we collect?

Personal information may include: your name, contact details, date of birth, other identification details, emergency contact details, medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors; Medicare number (where available) for identification and claiming purposes; healthcare identifiers; health fund details; bank account and/or credit card details, and payment history.

How do we collect your personal information?

We collect your personal information in the following ways:



- When you become a patient, you will be required to supply personal and demographic information, as well as health information such as allergies, health, and family history.
- When you make an appointment online or over the phone, credit card details are required to secure your appointment.
- Credit card details are entered directly into our appointment booking software Automated, which is integrated with Tyro, an Australian merchant bank. Rotem Medical Family Practice does not store your credit card details and instead uses a secure encrypted token provided by Tyro.
- During your care, additional information may be collected.
- We may collect information when you visit our website, contact us electronically, telephone us, make an online appointment or interact with us on social media.
- In some cases, we may collect information from:
 - Your guardian or responsible person;
 - Other healthcare providers (e.g., specialists, allied health professionals);
 - Hospitals, community health services, pathology, and diagnostic imaging services;
 - Medicare, your health fund, or the Department of Veterans' Affairs.

Various types of images may be collected and used, including:

- **CCTV footage:** For the safety of staff, contractors, lessees, patients, and visitors, CCTV cameras have been installed. Signage informing staff, patients and visitors is visible on entering the reception area. CCTV footage is stored on site with footage being archived for 24 days. CCTV footage may be disclosed as part of a police investigation to investigate or prevent crime in the Practice. The consent of individuals may not be required if access to the footage is reasonably necessary to a police investigation.
- **Photos and medical images:** Photos and images may be taken, when appropriate and necessary, for the purpose of patient management and are stored in the patient health record. Photos may be taken using personal devices and are immediately uploaded to the patient file and then destroyed on the personal device. Photos and images for health management reasons are only taken after informed consent is gained by the patient.

Sharing your personal information

In some circumstances, we may be required to share your personal information. However, only people who need to access your information will be able to do so.

We may share your personal information:

- With other healthcare providers to coordinate your care and prepare health documentation including Shared Health Summaries and Event Summaries for My Health Record;
- In emergency situations to lessen or prevent a serious threat to your life, health or safety, or to public health or safety;



- With your emergency contact if you are unable to act on your own behalf;
- If required or authorised by law (e.g. court subpoenas);
- To assist in locating a missing person;
- To establish, exercise or defend an equitable claim;
- As part of a confidential dispute resolution process;
- In case of mandatory disease notification;
- With third parties for business purposes (e.g., accreditation agencies, IT providers), provided they comply with Australian Privacy Principles.

We will not disclose your personal information outside Australia without your consent, unless required or permitted by law.

How do we store and protect your personal information?

Your information is primarily stored in a secure electronic health record. Any paper documents that may be received are scanned immediately to the patient record and are shredded on site. If paper records are held on site, they are kept in a cupboard under lock-and-key. Credit card data is not stored by Rotem Medical Family Practice; it is stored securely by Tyro using bank-grade encryption. Security measures include:

- Secured premises;
- Password protection and access controls on electronic systems;
- Two-factor authentication on log-ins to devices and software
- Private, secure environments for telehealth consultations.

We take reasonable steps to ensure your personal information is accurate and current. You may be asked to confirm your details at each visit. Rotem Medical Family Practice requires its employees to observe obligations of confidentiality in the course of their employment with all staff/contractors signing Confidentiality Agreements.

How long do we keep your personal information?

We retain personal health information in accordance with NSW health record retention laws. When information is no longer needed, we securely destroy or de-identify it, unless required by law to retain it longer.

How can you access and correct your personal information at Rotem Medical Family Practice?

You have the right to request access to, and correction of, your personal information. All requests for access to personal information must be made in writing via the Contact Us portal on the website, and we will respond within a reasonable time. Rotem Medical Family Practice takes all reasonable steps to maintain the accuracy of your personal information. We will ask you to verify that the personal information we hold about you is correct and current whenever you contact or attend the practice. You may also request that we correct or update your information, and you should make such in writing by email. We may deny access to your medical records in certain circumstances permitted by law, for example, if



disclosure may cause a serious threat to your health or safety. We will always tell you why access is denied and the options you have to respond to our decision.

My Health Record

You can choose whether or not to participate in the My Health Record system. If you wish to opt-out or manage your preferences, please visit www.myhealthrecord.gov.au.

Dealing 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.

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 may use document automation technologies to assist in the preparation of referral letters, care plans, and other clinical correspondence. These technologies are used to improve efficiency and support the accuracy and consistency of clinical documentation. Any documents generated with the assistance of these technologies are reviewed and approved by your treating Healthcare Practitioner before they are finalised or shared. We take reasonable steps to ensure that only the personal and health information necessary for the intended purpose is included in any clinical correspondence. 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](#).

Use of Artificial Intelligence (AI)

Our Healthcare Practitioners may use artificial intelligence (AI) tools to assist in delivering healthcare services and improving practice efficiency. This may include recording, transcribing, summarising, or preparing clinical notes and other clinical documentation during or after your consultation. AI will only be used with your prior consent, and you may decline or withdraw your consent at any time without affecting the healthcare you receive. Your Healthcare Practitioner remains responsible for your clinical care and will review and verify the accuracy of any AI-generated information before it is relied upon or included in your medical record. All AI tools used by our Healthcare Practitioners are expected to comply with applicable privacy legislation, professional standards, and ethical obligations to ensure your personal and health information is handled securely and appropriately.



Privacy and our website

Any information collected through our website is treated confidentially and stored securely. If we use cookies, analytics or third-party tracking tools, this will be disclosed on the website and you will be provided with options to manage your preferences.

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

Rotem Medical Family Practice take complaints and concerns regarding privacy seriously. If you have any concerns about the privacy of your information (including complaints about our use of the My Health Record system), please contact us by writing. Upon receiving your complaint, we will consider the details and attempt to resolve it in accordance with our complaints handling procedures.

If you would like to communicate with the practice anonymously, there is a patient feedback form at the reception desk and on our website. You may also contact the OAIC regarding privacy concerns. Generally, the OAIC will require you to give them time to respond before they will investigate. For further information visit www.oaic.gov.au or call the OAIC on 1300 363 992.

Notifiable Data Breach

The notifiable Data Breaches (NDB) scheme under Part IIIIC of the Privacy Act 1988 (Privacy Act) establishes requirements for entities in responding to data breaches. Entities have data breach notification obligations when a data breach is likely to result in serious harm to any individuals whose personal information is involved in the breach.

Policy review statement

This Privacy Policy is current from June 2026 and is reviewed annually. From time to time, we may make changes to our policy, processes and systems in relation to how we handle your personal information. We will update this Privacy Policy to reflect any changes. Those changes will be available on our website and in the practice.