



Thrive Family Practice Privacy Policy

Current as of: 22nd July 2024

To be reviewed 22nd July 2025

Introduction

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.

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 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, this includes recording, duplication and storage of consultations carried out via telehealth or remotely.

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

Our practice will need to collect your personal information to provide healthcare services to you. Our main purpose for collecting, using, holding and sharing your personal information is to manage your health. We also use it for directly related business activities, such as financial claims and payments, practice audits and accreditation, and business processes (eg staff training).

What personal information do we collect?

The information we will collect about you includes your:

- names, date of birth, addresses, 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.

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.

How do we collect your personal information?

Our practice may collect your personal information in several different ways.

1. When you make your first appointment our practice staff will collect your personal and demographic information via your registration.
2. During the course of providing medical services, we may collect further personal information.

Information may also be collected through Electronic Transfer of Prescriptions, (eTP), My Health Record, eg via Shared Health Summary, Event Summary.

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.

3. In some circumstances personal information may also be collected from other sources. Often this is because 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, community health services and pathology and diagnostic imaging services
 - your health fund, Medicare, or the Department of Veterans' Affairs (as necessary).

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

We sometimes share your personal information:

- with third parties who work with our practice for business purposes, such as allied health providers, accreditation agencies or information technology providers such as our online appointment provider (Hot Doc) these third parties are required to comply with APPs and this policy
- with other healthcare providers
- when it is required or authorised by law (eg 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 there is a statutory requirement to share certain personal information (eg some diseases require mandatory notification)
- during the course of providing medical services, through eTP, My Health Record (eg via Shared Health Summary, Event Summary).
- Only people who 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 may use your personal information to improve the quality of the services we offer to our patients through research and analysis of our patient data.

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.

We may provide de-identified data to other organisations to improve population health outcomes. The information is secure, patients cannot be identified, and the information is stored within Australia. You can let our reception staff know if you do not want your information included.

What information is held on a patient health record?

Information, held about a patient, in paper form or electronic form, which may include:

- contact and demographic information
- medical history
- notes on treatment
- observations
- correspondence
- investigations
- test results photographs
- prescription records
- medication charts
- insurance information
- legal information and reports
- work health and safety reports

How does the practice use automation technologies

When referrals are sent the practice uses automated technologies and only relevant information related to the care of the patient is included.

How do we store and protect your personal information?

Our practice stores all personal information securely in electronic format, on password protected systems.

We use a private cloud base system. Our server is in Adelaide and only accessible by our Information Technology company. There is one person only with access to this system.

Our practice stores all personal information securely.

Each person with access to our computer system signs a confidentiality agreement to ensure your personal and sensitive details remain confidential and are not discussed by any third party.

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.

Our practice acknowledges patients may request access to their medical records. We require you to put this request in writing. Please ask our reception staff for an authority form. Our practice will respond within 30 days. Fees may apply for copies of notes in excess of 20 pages.

Our practice will take reasonable steps to correct your personal information where the information is not accurate or up to date. From time-to-time, we will ask you to verify your personal information held by our practice is correct and up to date. You may also request that we correct or update your information. This can either be done in person via the reception staff or via a letter addressed to the

Practice Manager, Thrive Family Practice, 88A Partridge Street Glenelg South SA 5045.

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

We take complaints and concerns regarding privacy seriously. Should you have any concerns. Please ask to speak with Sharon, our Practice Manager or you can express any privacy concerns you may have in writing. We will then attempt to resolve it in accordance with our resolution procedure. Please post your letter to Thrive Family Practice 88A Partridge Street Glenelg South SA 5045. We will endeavor to respond within 30 days.

You may also contact the OAIC. Generally, the OAIC will require you to give them time to respond before they investigate. For further information visit www.oaic.gov.au or call the OAIC on 1300 363 992.

Privacy and our website

We will never place any personal patient information on our website or social media pages. Your details will not be disclosed to a third party without your consent.

Handling of Human Error Leading to a Privacy Breach

We acknowledge that human error can occasionally result in unintentional breaches of patient privacy, such as the accidental sharing or exposure of personal or health information. Our practice has implemented the following procedures to manage these incidents:

Minor Breach

A **minor breach** is defined as a breach where the potential impact on the patient is considered low and is limited in scope (e.g., an email containing patient details is accidentally sent to a colleague).

Actions:

- The staff member involved must immediately inform the Practice Principal and Practice Manager.
- Details of the breach are to be recorded and stored securely in a dedicated folder held by the Practice Manager.
- The staff member responsible will be given a copy of the recorded breach and a recommendation to personally contact the affected patient. The patient should be informed of the breach, offered an apology, and consulted on any further steps needed to ensure their privacy is protected.
- Any remedial actions should be documented, and staff training will be reviewed to prevent further occurrences.

Major Breach

A **major breach** involves a more serious exposure of personal information, with the potential for greater harm to the patient (e.g., sharing information with a third party not involved in the patient's care).

Actions:

- The Practice Principal, Practice Manager, and the involved staff member will convene to assess the situation. If necessary, the clinic will consult with its medical insurer to obtain legal advice.
- A strategy for approaching and informing the patient will be developed, which may include a formal letter, in-person meeting, or other appropriate forms of communication.
- The breach will be logged with the Office of the Australian Information Commissioner (OAIC) in accordance with the Notifiable Data Breach (NDB) scheme, if applicable.
- Affected parties will be informed of the breach and the steps taken to mitigate any risks.
- An internal review of policies, procedures, and staff training will be conducted to ensure the breach does not reoccur.

In the event of a Data Breach

Our clinic has an obligation under the Privacy Act to secure personal information and we must comply with the Notifiable Data Breach (NDB) scheme.

Thrive Family Practice has done its due diligence to ensure that our team are appropriately trained and kept up to date in all areas of privacy and confidentiality. Our systems are rigorously tested and updated to ensure that all data held on the premises is kept safe.

In the event of a suspected or confirmed data breach of personal information, our management team, along with our IT expert, will liaise with OAIC to establish the cause of the breach, what information has been affected, who has been affected and what steps need to be taken to advise all persons affected, which may include our patients and stake holders.

Policy review statement

This policy will be reviewed annually to ensure it is in accordance with any changes that may occur. Changes will be published on our website.

Disclaimer

The *Privacy policy template for general practices* is intended for use as a guide of a general nature only and may or may not be relevant to particular practices or circumstances. The Royal Australian College of General Practitioners (RACGP) has used its best endeavours to ensure the template is adapted for general practice to address current and anticipated future privacy requirements. Persons adopting or implementing its procedures or recommendations should exercise their own independent skill or judgement, or seek appropriate professional advice. While the template is directed to general practice, it does not ensure compliance with any privacy laws, and cannot of itself guarantee discharge of the duty of care owed to patients. Accordingly, the RACGP disclaims all liability (including negligence) to any users of the information contained in this template for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of reliance on the template in any manner.