

Privacy Policy and Consent

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, practitioners 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.

We take your care and your information privacy seriously. In order to thoroughly assess, diagnose and provide therapy, we need to collect some personal information from you. This will support us to provide you with a high quality, holistic service. This information is provided at your discretion but if you do not provide this information; we may be unable to treat you.

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).

In summary your information will be used for:

- The provision of high quality care to you which may at times require disclosure of information to other practitioners within the practice to ensure ongoing care or to your doctors or other professionals involved in your care
- The administrative purpose of running the practice
- Billing - either directly or through a private health insurer, Medicare, Department of Veterans Affairs or compensation agency eg Workcover
- In the case of insurance or compensation claim it may be necessary to disclose and/or collect information that concerns your return to work to an insurer or your employer

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. Please advise the client services team if you wish to do so.

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 over the phone and then via your new patient intake form.
2. During the course of providing medical services, we may collect further personal information.
For example through electronic transfer of prescriptions (eTP), My Health Record, Shared Health Summary, Event Summary. Unless you have opted out or provided written instructions that do not wish to participate we may upload your GP records to My Health Record.
3. 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.
4. 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 accreditation agencies or information technology providers – these third parties are required to comply with APPs and this policy
- with other healthcare providers – only information relevant to your current condition is shared for the purposes of treatment of the current condition.
- 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). Unless you have opted out or provided written instructions that do not wish to participate we may upload your GP records to My Health Record.
- As required by law, or
- Under other circumstances where permitted under the Privacy Act.

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.

Marketing

Our practice may use your email address to market our goods or services directly to you from time to time. You may opt out of direct marketing at any time.

Information Security

We take your privacy seriously and therefore we have the following security measures in place to store and protect your personal information:

- We do not disclose your personal information to anyone other than as stated above
- Your information is stored electronically and protected by bank-grade security and encryption
- All team members are educated on data protection procedures and password safety management.
- Secured data centres to store data.
- Personal Data Breach Protocol for quick and efficient reactions in case of suspicion of data being compromised.
- Access to account is secured by login, passwords.
- Each user has their own access and is instructed on risk of sharing access.
- Detailed permission setting for each staff member to control each section and task user can access.
- Database require login after short time of inactivity.
- All activity within the database is logged.

Information Storage and Security

Saltfleet Clinic is committed to personal information being managed confidentially and securely.

We use Nookal Practice Management Software and Best Practice to store personal information, clinical notes and billing records. Your personal information can only be accessed by our staff with their unique username and password that gives them a level of access specific to their role.

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.

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 that your personal information held by our practice is correct and current. You may also request that we correct or update your information, and you should make such requests in writing to info@saltfleetclinic.com.au

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. You should express any privacy concerns you may have in writing:

info@saltfleetclinic.com.au

or

15 Saltfleet St
Port Noarlunga
SA 5167

We will then attempt to respond to your complaint within 30 days.

You may also contact the OAIC. 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.



Privacy and our website

No personal information is requested nor stored through our website, other than when you make a booking via our website. We use analytics to measure site traffic.

Policy review statement

This privacy policy will be reviewed regularly to ensure it is in accordance with any legislative changes that may occur. Changes will be incorporated into the policy.

Policy Availability

We will make our privacy policy available upon request and will provide a link to this policy from our website.

Policy Review

This policy will be reviewed annually. Next Review July 1 2020.