NORTHAM FAMILY PRACTICE PRIVACY POLICY

Current as of: January 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.

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 primary 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 (e.g. 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

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.
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
- when it is required or authorised by law (e.g. 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 (e.g. some diseases require mandatory notification)
- during the course of providing medical services, through eTP, My Health Record (e.g. 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 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.

How do we store and protect your personal information?
Your personal information is stored in our practice by electronic records.
Our practice stores all personal information securely and we ensure your information is protected to the highest degree. We have a password/ username system for our medical software program as well as our IT has set up extensive security settings on our network. All staff has signed a confidentiality agreement before commencing work.

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 that patients may request access to their medical records. We require you to put this request in writing and signed our release of medical records form. Our practice will respond within a reasonable time; this could take up to 1 week depending on if your usual doctor is available to approve the release. There may be fees involved in the release of your medical records; please discuss this with reception.
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 us.

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. We will then attempt to resolve it in accordance with our resolution procedure. Complaints can be lodged in writing to the Practice Manager at

p.manager@jupiterhealthsubiaco.com.au. We attempt to respond to complaints in a reasonable time frame but on occasions this may take up to 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 or call the OAIC on 1300 363 992.

Privacy and our website
Collection of information

Two types of online data are collected:

- visitor logs and statistics
- information provided by users through online forms, registration, databases, and feedback (when personal information is collected online through databases and forms, for example, a privacy notice information will be collected, user and protected will be available.

Visitor logs and statistics
The main purpose for collecting this information is to provide statistical information used for website and system administration. The information does not identify individual users but does identify the computer that is used to access our sites.
Logged information is not disclosed outside of our organisation. We do not attempt to identify individuals from these records unless it is necessary to the investigation of a breach of law.

How do we use document automation technologies?
As we ensure that your privacy always remains our utmost concern, Electronic Documents generated by our practice such as referrals, medical certificates, etc. utilise appropriate and secure document automation technologies.
Our Practice utilise a secure medical software, which has a word processing application to generate documents as and when required. This Word processing application has algorithms to automatically import strictly relevant medical information only, required for the patient and for the documentation.
The medical software has proper security authentication protocols with unique user credentials which can only be accessed by authorised Practice staff according to their roles and responsibilities.

Consent telehealth consultations- Once clinical appropriateness is confirmed and the patient and GP have decided to proceed, seek prior consent from the patient and document this in the patient's health record held by the practice. Seek consent from patients prior to a consultation if a third party will be present during the consultation at either the specialist or patient end of a consultation. Document such consent in the patient's health record held by the practice

Policy review statement
Our privacy policy is reviewed regularly to ensure it is in accordance with any changes that may occur. Updates of any changes can be found on our website.
Last Reviewed: January 2025.