Donnybrook Family Doctors Privacy Policy

Donnybrook Family Doctors

Privacy Policy

Document owner: Iminder Nandha (Practice Manager)

Approved by: Dr. Nina Nandha (Practice Principal)

Version: 1.1

Effective date: 05 / 04 / 2026

Review date: 05 / 04 / 2027

Introduction

Donnybrook Family Doctors ("the practice", "we", "our", "us") is committed to protecting the privacy and confidentiality of all personal and health information we collect.

This Privacy Policy explains how we collect, use, disclose, store and protect your personal and health information. It applies to patients, prospective patients, visitors to the practice and users of our website.

Our practice complies with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the My Health Records Act 2012 (Cth), applicable Western Australian legal requirements and the current RACGP Standards for general practices applicable to our accreditation cycle.

What Is Personal and Health Information?

"Personal information" means information or an opinion about an identified, or reasonably identifiable, individual.

"Health information" is a type of sensitive personal information. It includes:

- Information about your physical or mental health, illnesses, injuries or disabilities
- Information about health services you have received or wish to receive
- Personal information collected to provide a health service
- Genetic information that could be predictive of your health
- Other information about your health that is reasonably obtained in the course of providing care

Information We Collect

The personal and health information we may collect about you includes:

- Your full name, date of birth and gender
- Your home, postal and email addresses
- Phone numbers (home, mobile, work)
- Medicare number, Department of Veterans' Affairs (DVA) number, pension or concession card details and private health insurance details
- Next of kin and emergency contact details
- Your medical history, current medications, allergies, immunisation status and family medical history
- Test results, referrals, hospital discharge summaries, specialist letters and imaging reports
- Notes from consultations and clinical observations
- Information about appointments, recalls and reminders
- Billing, payment and Medicare claim details
- Aboriginal or Torres Strait Islander status, where you choose to provide it, so we can offer culturally appropriate care and access relevant Medicare items
- Photographs or images, where clinically relevant and with your specific consent (for example, of skin lesions for monitoring)

Where it is lawful and practicable, you may interact with us using a pseudonym or anonymously — for example, when seeking general information. Most clinical care, however, requires us to know your identity to ensure your safety, claim Medicare benefits and meet our legal obligations.

How We Collect Your Information

We collect your information directly from you wherever possible. This includes when you:

- Register as a new patient or update your details
- Speak with reception in person, by phone, or via secure messaging
- Attend a consultation with a doctor, nurse or other practitioner
- Book an appointment online (for example, via HotDoc)
- Send us correspondence, complete a form, or provide consent

We may also collect information about you from third parties, including:

- Your treating specialists, hospitals, pathology providers and imaging providers
- Other general practices, where you transfer your care to us
- Your nominated representative, parent, guardian or carer
- Medicare, the DVA, the Australian Immunisation Register and the My Health Record system

- WorkCover insurers and other third-party funders, where they relate to a claim

We will only collect information from third parties where you have consented, where it is necessary for your healthcare, or where it is otherwise authorised or required by law.

How We Use and Disclose Your Information

We use and disclose your information for the primary purpose of providing healthcare to you, and for related secondary purposes you would reasonably expect, including:

- Communicating with other healthcare providers involved in your care, such as specialists, hospitals, allied health providers, pathology and imaging providers
- Processing Medicare, DVA and private health insurance claims
- Sending recalls, reminders and clinically important results
- Maintaining and auditing your medical record
- Quality improvement, accreditation and clinical audit activities
- Teaching and training of medical, nursing and allied-health students or registrars, where you have consented
- Reporting notifiable diseases, births, deaths and other matters required by law
- Responding to subpoenas, court orders or other lawful requests

We will not use or disclose your health information for any other purpose without your consent, unless the disclosure is required or authorised by law, or is necessary to lessen or prevent a serious threat to life, health or safety.

We may disclose necessary health information to a parent, guardian, carer, substitute decision-maker or responsible person where you have consented, where it is necessary for your healthcare, where you are unable to consent or communicate consent, or where disclosure is otherwise required or authorised by law.

My Health Record

Where you have a My Health Record and have not opted out, we may, with your consent and where clinically appropriate, view information uploaded by other providers and upload information from our practice (for example, shared health summaries, event summaries and prescription records).

You can change your access controls or remove documents from your My Health Record at any time. Speak with your doctor or visit www.myhealthrecord.gov.au if you have questions.

Data breaches involving the My Health Record system will be managed in accordance with the My Health Records Act 2012 and applicable mandatory notification requirements.

Communicating With You

We may contact you by phone, SMS, letter, email or secure electronic message about your healthcare, including appointment reminders, recalls, results and health information.

Email and SMS are not fully secure forms of communication. By providing us with your email and mobile number you consent to us communicating with you using those channels for healthcare-related matters. You can opt out of non-essential communication at any time by contacting reception — however, some communication may be required for clinical safety, such as urgent results or recalls.

Where appropriate, we use secure messaging systems such as HealthLink to exchange clinical information with other providers.

Referral Letters and Automated Documents

Our clinical software may use templates or automated functions to generate referrals, letters, recalls, reminders and other clinical documents. Clinicians are responsible for checking documents before they are sent to ensure they are accurate and contain only information relevant to the purpose of the communication.

Direct Marketing

We do not sell your information. We do not use your health information to send you advertising or marketing material from third parties. From time to time we may send you information about practice services, public-health campaigns, vaccination programs or preventive-health initiatives. You can opt out of these communications at any time by contacting reception.

Storage and Security of Your Information

We take reasonable steps to protect your information from loss, misuse, interference, unauthorised access, modification or disclosure. These steps include:

- Storing electronic health records in our secure clinical software (Best Practice) with role-based user access and individual user accounts
- Securing paper records in locked cabinets, accessible only to authorised staff
- Storing prescription forms, practice letterhead, administrative templates, official documents and other controlled documents securely, with access limited to authorised team members
- Using encrypted secure messaging for clinical correspondence between providers, where available
- Backing up electronic records regularly and storing backups securely
- Maintaining up-to-date anti-virus, firewall and operating-system protections on practice computers

- Requiring all staff, doctors, students and contractors to sign confidentiality agreements and to complete privacy awareness training
- Maintaining audit logs of access to electronic records

If we become aware of a data breach that is likely to result in serious harm, we will respond in accordance with the Notifiable Data Breaches scheme, which may include notifying you and the Office of the Australian Information Commissioner.

Access to Your Health Information

You have the right to request access to the personal and health information we hold about you. Requests should be made in writing to the Practice Manager.

We will respond to your request within a reasonable period, generally within 30 days. We may charge a reasonable fee for the time taken to retrieve, copy or transfer records. We will let you know any fees before processing your request.

In limited circumstances, we may need to refuse access — for example, where giving access would pose a serious threat to life, health or safety, or where the request is frivolous or vexatious. If we refuse, we will give you our reasons in writing and explain how to complain.

Correction of Your Information

If you believe the information we hold about you is inaccurate, out of date, incomplete, irrelevant or misleading, you can ask us to correct it. We will take reasonable steps to correct the information, or to attach a statement to the record noting your concerns where correction is not possible (for example, where the original entry forms part of a clinical history).

Please advise reception promptly of any change to your name, address, phone, email, emergency contact, Medicare or concession-card details so that we can keep your record current.

Retention and Destruction of Records

We retain medical records for the period required by law. In Western Australia, adult records must generally be kept for at least seven years from the date of last entry. Records of patients who were under 18 at the time of the last entry are kept until the patient turns 25, or for seven years after the last entry, whichever is longer.

When records are no longer required, we destroy or de-identify them in a secure manner.

Transfer of Records to Another Practice

If you transfer your care to another medical practice, you may request a copy or summary of your health record be sent to your new treating doctor. Requests must be made in

writing and signed by you or your authorised representative. A reasonable fee may apply for copying, printing or transferring records.

Disclosure to Overseas Recipients

We do not routinely disclose your information to overseas recipients. If we do use a service provider that stores or processes data outside Australia (for example, a cloud-based clinical or administrative service), we will take reasonable steps to ensure that recipient handles your information consistently with the Australian Privacy Principles.

Photographs, Video and Social Media

We will only photograph or video record you where it is clinically necessary (for example, monitoring a skin lesion) and with your specific written consent. Such images are stored in your medical record under the same protections as the rest of the record.

Audio or video recording of consultations, including telehealth consultations, must not occur without the knowledge and consent of all relevant parties. Any clinically required recording, photograph or image will be managed as part of the patient's health record.

We will not publish identifiable images of patients on our website, social media or marketing material without separate, informed and written consent. You can withdraw consent at any time.

Children and Young People

For children under 14, parents or legal guardians generally provide consent for treatment and access to records. From around 14 years of age, young people may be considered “mature minors” and able to consent to their own care and to control access to their records, depending on their understanding and the circumstances.

Our doctors and nurses make these assessments on a case-by-case basis, in line with current Australian guidance, and may discuss them with the young person privately.

Privacy Complaints

If you believe your privacy has been breached, please raise the matter with us first so we can try to resolve it:

Practice Manager: Iminder Nandha

Email: manager@dfdoctors.com.au

Phone: (08) 9731 1888

Postal address: 92 South Western Highway, Donnybrook WA 6239

We will acknowledge your complaint promptly and aim to investigate and respond within 30 days.

If you are not satisfied with our response, you may contact:

Office of the Australian Information Commissioner (OAIC):

Phone: 1300 363 992

Website: www.oaic.gov.au

Health and Disability Services Complaints Office WA (HaDSCO):

Phone: 1800 813 583

Website: www.hadsco.wa.gov.au

Changes to This Policy

We review this Privacy Policy at least annually and update it as our practices, technologies or legal obligations change. The current version is available on our website (www.donnybrookfamilydoctors.com.au) and at reception. The version number and effective date on the cover page indicate the latest update.

Contact Us

If you have questions about this Privacy Policy or how we handle your information, please contact:

Donnybrook Family Doctors:

92 South Western Highway, Donnybrook WA 6239

Phone: (08) 9731 1888

Fax: (08) 9731 1889

Email: info@dfdoctors.com.au

Website: www.donnybrookfamilydoctors.com.au

Document Control

Version: 1.1

Effective date: 05 / 04 / 2026

Review date: 05 / 04 / 2027

Document owner: Iminder Nandha (Practice Manager)

Approved by: Dr. Nina Nandha (Practice Principal)

Next review: Annual, or sooner if practice details, legislation or RACGP Standards change