

Privacy Policy

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 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 consult notes, medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors.
- Information collected through AI-assisted clinical documentation tools, including transcriptions and draft clinical notes generated with patient consent.
- Medicare number (where available) for identification and claiming purposes.
- healthcare identifiers.
- health fund details.

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, which may include electronic transfer of prescriptions (eTP), My Health Record, e.g. via Shared Health Summary, or Event Summary.
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 via HotDoc.

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).
5. During consultations where consent has been obtained, information may be collected through approved AI-assisted clinical transcription tools used to support clinical documentation.

Artificial Intelligence (AI) Assisted Clinical Documentation

The practice may utilise approved artificial intelligence (AI) tools, including clinical documentation and transcription software, to assist practitioners during consultations.

These tools may be used to transcribe conversations between patients and practitioners and generate draft clinical notes to support the provision of healthcare services. All clinical records are reviewed, verified, and approved by the treating practitioner before being entered into the patient's health record. The treating practitioner remains responsible for the accuracy, completeness, and clinical appropriateness of all information entered into the patient's health record.

The practice only uses AI applications that are intended for healthcare settings and that incorporate appropriate privacy, security, and confidentiality safeguards.

Where AI-assisted transcription is used, patient consent will be obtained and documented in the patient's health record. Patients may decline or withdraw consent for the use of AI-assisted transcription at any time without affecting their access to care.

Information processed through AI applications is managed in accordance with applicable privacy legislation, the practice's privacy and information security policies, and the provider's privacy obligations.

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 Australian Privacy Principles (APPs) and this policy.
- with other healthcare providers.
- when it is required or authorised by law (e.g. court subpoenas and Direction of production).
- 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.

Taken from: [Policy and Procedure Manual – UCD-HCD](#)

Version: 2.0

Effective Date: 13/10/2026

Next Review Date: 13/10/2027

- 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.

Except where required for the provision of approved healthcare technology services and permitted by law, the practice will not disclose personal information outside Australia 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.

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.

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.

Electronic Communication and Secure Transmission of Information

The practice may communicate with patients electronically for administrative purposes and to provide healthcare-related information where appropriate.

Electronic communications may include email, SMS correspondence, electronic prescriptions (eScripts), referrals, health summaries, and other healthcare-related documents.

The practice uses encrypted email systems and applies security measures to protect information transmitted electronically.

Where clinical or medical documents are sent electronically, attachments are password protected to enhance security and confidentiality. Passwords are generally based on the patient's date of birth in DDMM format unless alternative arrangements are required.

Prior to sending information electronically, the practice verifies the patient's nominated contact details to ensure information is sent to the intended recipient.

While the practice takes reasonable steps to protect information transmitted electronically, patients should be aware that electronic communication carries inherent security risks that cannot be completely eliminated.

The practice email addresses are intended for administrative communication only and should not be used for:

- Seeking medical advice
- Requesting prescriptions
- Requesting referrals
- Booking, cancelling or changing appointments
- Communicating urgent medical concerns

Patients requiring these services should contact the practice directly by phone.

How do we store and protect your personal information?

Your personal information may be stored in various forms, including electronic health records, visual records (such as X-rays, scans, photographs and videos), correspondence, and other clinical documentation.

Our practice stores personal information securely using protected clinical information systems and secure electronic storage environments. Access to patient information is restricted to authorised personnel involved in your care or the operation of the practice and is controlled through individual user accounts, passwords, and role-based access permissions.

To protect patient privacy and confidentiality, the practice implements a range of physical, administrative, and technical security measures, including:

- Individual usernames and passwords for all staff members.
- Automatic screen locking and password-protected devices.
- Secure access controls and restricted access areas.
- Encrypted email communications.
- Password-protected clinical documents transmitted electronically.
- Secure backup and information management systems.
- Staff confidentiality agreements and privacy training.
- Secure destruction of confidential information and storage media when no longer required.
- CCTV monitoring of practice premises where appropriate.
- Secure storage of paper-based records and confidential documents.
- Routine review of user access permissions.

All members of the practice team are required to maintain the confidentiality of patient information and access only the information necessary to perform their duties.

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 and our practice will respond within 30 days. A basic Health Summary can be provided at no cost. If you require a copy of your entire medical record (including all Consultation Notes, Test Results and Specialist Letters), a fee of \$60 may apply for the preparation and provision of a full copy of the medical record, subject to applicable privacy legislation and practice policies.

Appropriate security measures are applied to protect the confidentiality of medical records during transmission. Depending on the method of delivery, records may be sent as password-protected attachments, via a secure password-protected OneDrive link, or provided through another secure electronic transfer method approved by the practice.

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 administration via email, for UCD: admin@ucdrs.com.au or HCD: admin@horsleycommunitydoctors.com.au

Disposal of Information

The practice takes reasonable steps to securely dispose of personal information that is no longer required.

Paper records and confidential documents are destroyed using a cross-cut shredder. Electronic storage media containing patient information, including USB drives, CDs, and other removable storage devices, are securely erased, reformatted, or physically destroyed prior to disposal. These processes are undertaken to minimise the risk of unauthorised access, disclosure or loss of patient information.

Data Breaches

The practice has procedures in place to identify, investigate, contain, and respond to actual or suspected privacy breaches and data security incidents. Where a data breach is likely to result in serious harm, the practice will comply with its obligations under the Notifiable Data Breaches Scheme, including notification to affected individuals and the Office of the Australian Information Commissioner (OAIC) where required by law.

Privacy Officer

The Practice Manager, Dr Priyank Gupta, and Dr Priyanka Singh act as Privacy Officers and are the primary contacts for privacy-related enquiries, access requests, corrections, and complaints.

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

All privacy complaints, investigations, correspondence, actions taken, and outcomes are documented and retained by the practice in accordance with the complaints management process.

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. Please email practice.manager@horsleycommunitydoctors.com.au regarding your concern or send a handwritten complaint to:

Unanderra Community Doctors
33 Farmborough Road,
Unanderra, NSW, 2526
Ph: (02) 4204 9734

Horsley Community Doctors
44 Horsley Drive,
Horsley, NSW, 2530
Ph: (02) 4208 3650

The practice will endeavour to acknowledge complaints promptly and aims to provide a resolution within 30 days where reasonably practicable.

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. Alternatively, you may contact:

NSW Health: Health Care Complaints Commission
Locked Mail Bag 18
Strawberry Hills NSW 2012
Ph: (02) 9219 7444
F: (02) 9281 4585
Email: hccc@hccc.nsw.gov.au
Website: www.hccc.nsw.gov.au

Policy review statement

This policy will be reviewed annually, or sooner if legislative, technological, privacy, information security, or operational changes occur.

An updated version of this privacy policy will be made available at reception, and a copy can be requested at any time.

Appendix A - Patient Complaint Form

The following form is used by the practice to document, investigate, manage, and resolve complaints in accordance with the practice complaints management procedure.

Staff member taking complaint	
Name (printed):	Signature:

How was the complaint made? (e.g. phone, in person, letter)		
Description:		
Date:	Time:	Location in practice:

Details of complainant	
Complainant name:	File ID:
Address:	Phone:

Description of complaint (from complainant's point of view)		
☐ Privacy	☐ Other Health Issue	Date:
Description:		

What action was taken?		
Description:		
Incident form completed?	☐ Yes	☐ No

Practice Manager/Practice Principal notification:	Date:	Time:
Date complaint acknowledgement letter sent:	☐ Yes	☐ No

Situation Resolution		
Situation resolved?	Date: ☐ Yes	☐ No
If no, referred further action to:	☐ National Privacy Commissioner	☐ Health Services Commissioner
Referred for discussion at Practice meeting:	☐ Yes	☐ No