

Only people who need to access your information will be able to do so. Other than while 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 may be stored at our practice in various forms. Such as electronic records, visual records (X-rays and CT scans).

Our practice stores all personal information securely. Such as in a protected information system, in hard copy format in a secured environment We use passwords, secure cabinets and confidentiality agreements for staff and contractors

Real—time audio/visual recording and duplication and storage of a consultation, including those via telehealth and those conducted remotely never occurs without first obtaining the patient's consent which is documented in the patient's file in our Best Practice Clinical Software.

#### **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. Please email our practice manager at

Practice.manager@hallroadmedicalcentre.com.au or post a letter to Hall Road Medical Centre T14, 100 Hall Road, Carrum downs, 3201 or phone us on 03 9783 0266 and we will endeavour to discuss, make change or correct the issue within 30 days.

#### **Further information on privacy legislation is available from:**

- Office of the Federal Privacy Commissioner  
1300 363 992
- Office of Health Services Commissioner (Vic)  
1800 136 066
- Community & Health Services Complaints Office (ACT) – 02 6205 2222
- Office of the NSW Privacy Commissioner  
02 9268 5588

You may also contact the OAIC, Office of the Australian Information Commission. Generally, the OAIC will require you to give them time to respond before they can get back to you.

#### **Practice Contact Details**

**Hall Road Medical Centre**

**T14, 100 Hall Road, Carrum Downs 3201**

**Phone: 03 9783 0266**

**Fax: 03 9782 0111**

**Email:**

**admin@hallroadmedicalcentre.com.au**



## **Practice Privacy Policy**

**Keeping your  
personal  
information  
private in our  
practice.**



Royal Australian College of General Practitioners

## **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 (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.

## **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
- Medications charts
- Insurance information
- Legal information and reports
- Work health and safety reports

## **How do we collect your personal information?**

Our practice may collect your personal information in several different ways. When you make your first appointment our practice staff will collect your personal and demographic information via your registration.

While providing medical services, we may collect further personal information. 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. 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).

## **How are document automation technologies used?**

Document automation is where systems use existing data to generate electronic documents relating to medical conditions and healthcare. The practice uses document automation technologies to create documents such as referrals which are sent to other healthcare providers. These documents contain only your relevant medical information. These document automation technologies are used through secure medical software Best Practice. All users of the medical software have their

own unique user credentials and passwords and can only access information that is relevant to their role in the practice team. The practice complies with the Australian privacy legislation and APPs to protect your information.

- All data, both electronic and paper are stored and managed in accordance with the Royal Australian College of General Practitioner's Privacy and maintaining health information guidance.

## **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 providing medical services, through eTP, My Health Record (eg via Shared Health Summary, Event Summary).

### **How do we ensure we securely manage our patient health information?**

Your personal information may be stored at our Practice in various forms.

- Our Practice stores information as electronic records (including via cloud-based services), visual records (including photos) and archived paper records.
- Our Practice stores all personal information securely via the use of passwords, encrypted back-ups, confidentiality agreements for staff and secure cabinets.
- All records will be retained until the later of seven (7) years from your last contact with the Practice, or until you reach the age of twenty-five (25).

- We take steps to destroy or de-identify information that we no longer require.
- Our server security policy is designed to protect the servers from unauthorised access, data breaches, and other security threats. Our Practice uses the following security measures to ensure the personal information which it holds is secured:
  - (a) Antivirus software is installed on all servers and updated regularly.
  - (b) Firewalls are configured to block unauthorised traffic.
  - (c) Servers are placed on their own subnet.
  - (d) Access to servers is restricted to authorised users.
  - (e) Physical access to the servers are limited, with servers located in a locked room and security cameras installed around the building.
  - (f) Servers are patched regularly to fix security vulnerabilities.
  - (g) Backups are created regularly every hour onsite with daily offsite backups

### **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. You can lodge this request either via email ([admin@hallroadmedicalcentre.com.au](mailto:admin@hallroadmedicalcentre.com.au)) or telephone. Our Practice will acknowledge your request within three (3) business days. We can post the requested information to your postal address, or we can email the information to you if you request it. If we are required to process a request for your records, we may charge for our reasonable costs incurred in complying with your signed request.

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 [admin@hallroadmedicalcentre.com.au](mailto:admin@hallroadmedicalcentre.com.au). There is no fee charged for making corrections to your personal information.

### **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 (including any breach of the Australian Privacy Principles ("APP") or any registered binding APP code) you may have in writing.

Complaints should be addressed to:

- (a) Name and Position: The Practice Manager
- (b) Address: T14, 100 Hall Road, Carrum Downs, 3201
- (c) Email: [practice.manager@hallroadmedicalcentre.com.au](mailto:practice.manager@hallroadmedicalcentre.com.au)

We will respond with acknowledgement of your complaint within three (3) business days and provide a response within thirty (30) business days.

You may also contact the Office of the Australian Information Commissioner ("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](http://www.oaic.gov.au) or call the OAIC on 1300 363 992.

## Privacy and our Website

If you “like” or comment on our social media pages, we will have your social media name.

Our website uses cookies. A “cookie” is a small file stored on your computer's browser, which assists in managing customised settings of the website and delivering content. We collect certain information such as your device type, browser type, IP address and pages you have accessed on our website and on third-party websites. You are not identifiable from such information. You can use the settings in your browser to control how your browser deals with cookies. However, in doing so, you may be unable to access certain pages or content on our website.

Our website may contain links to third-party websites. We are not responsible for the content or privacy practices of websites that are linked from our website

## Privacy statement review

This privacy policy will be reviewed annually to ensure it is in accordance with any changes that may occur.

Last reviewed: 20th March, 2026

## Policy review statement

This privacy policy is regularly reviewed to ensure compliance with current obligation.

If any changes are made:

- They will be reflected on the website
- Significant changes may be communicated directly to patients via email or other means. Please check the policy periodically for updates. If you have any questions, feel free to contact us.

## Patient Email Policy

### **Communicating via email to our patients**

Before communicating with a patient via email, we always ensure that we have obtained and documented our patient’s consent in their health records upon registration. Generally, our practice will only provide information that is of a general, non-urgent nature. Whilst not encouraged, our practice allows patients an opportunity to obtain advice or information related to their care by electronic means such as email but only where the general practitioner determines that a face-to-face consultation or telehealth appointment is unnecessary and agrees to communication by email. To maintain confidentiality, any email sent by the practice is encrypted through our Best Practice clinical software. The practice also uses an email disclaimer notice on outgoing emails that are affiliated with the practice stating: *This message is strictly confidential and should only be used by the intended addressee. If you are sent this message by error, please inform us immediately by phone and delete the document.*

### **Receiving email from our patients**

Note also that any information received by the patient is also used as a method to verify contact details we have recorded on file are current and up to date.

Our patients are fully informed that any information they chose to send is subject to risk that the information could be intercepted, read by someone other than the intended recipient and forwarded on.

As a practice, other professional and security measures we take are:

- Refrain from responding to unsolicited or unwanted emails
- Delete hoaxes or chain emails
- Emails from unknown senders are not opened
- Virus checking all email attachments
- Maintain appropriate professional language when communicating

## How are Artificial Intelligence (AI) Scribes used

The practice uses an AI scribe tool to support GPs take notes during their consultations with you. The AI scribe uses an audio recording of your consultation to generate a clinical note for your health record. The practice AI scribe service is Lyrebird Health.

### **Lyrebird Health:**

- **does/does not share information outside of Australia**
- **destroys/stores the audio file once the transcription is complete.** Storage Time By default, Lyrebird will only store your generated documentation for a default period of 7 days. After this period, the documentation, and associated transcript will be destroyed from our database.
- **removes/retains sensitive, personal identifying information as part of the transcription.** Encryption & Access If it is saved in Lyrebird, all information is stored on Lyrebird’s Australian Amazon Web Services (AWS) infrastructure, fully encrypted with bank level 256-bit encryption. This is the highest level of protection! No Third-Party Access Lyrebird Health’s Data Processing Agreement with all third parties ensures any data stored are only accessible to Lyrebird Health. No party can access or alter information. No Model Training on Your Data Lyrebird does not use your patient data to train our model, nor do we share it with anyone else. Your patient data is only accessible, and usable by you. Lyrebird is compliant with Privacy Act 1988, APP Principles & has been approved by the largest MDOs

**The practice will only use data from our digital scribe service to provide healthcare to you**