Optimal Health Medical Centre Privacy Policy

Current as of: 17/11/2025

Contents

Introduction

This policy explains how we collect, use, and protect your personal information, including your health information, and how we may need to share it to support your care. It outlines the situations where other healthcare providers or third parties may be involved, and the safeguards we apply when information is exchanged.

From December 2024, Australian privacy law defines personal information broadly. It now includes any data that can reasonably identify an individual, such as metadata and behavioural information. These obligations also extend to information received from organisations overseas or shared with service providers located outside Australia.

If you have questions or need more information, you can contact our Practice Manager at:

• Optimal Health Medical Centre Gregory Hills: (02) 4647 1133

• Optimal Health Medical Centre Rhodes Central: (02) 9189 1000

• Optimal Health Medical Centre Leppington: (02) 7200 8040

When and why is your consent necessary?

When you register as a patient, you provide informed consent for our GPs and practice staff to collect, access, and use your personal information so we can deliver safe, effective healthcare. Only team members who require access to your information to support your care or meet legal and clinical obligations are permitted to use it.

Your consent must be voluntary, current, and specific to the purposes outlined in this policy. By acknowledging this Privacy Policy, you consent to us collecting, holding, using, retaining, and disclosing your personal information as described.

If we need to use your information for any purpose not covered in this document, we will seek additional consent from you. You may withdraw your consent at any time by contacting the practice, noting that this may affect our ability to provide certain aspects of your care.

Why do we collect, use, store, and share your personal information?

The practice collects, uses, stores, and shares your personal information primarily to manage your health safely and effectively. This includes providing healthcare services, managing medical records, and ensuring accurate billing and payments. Additionally, we may utilise your information for internal quality and safety improvement processes such as practice audits, accreditation purposes, and staff training to maintain high-quality service standards.

What personal information is collected?

The information we will collect about you includes your:

- names, date of birth, addresses, contact details
- medical information including medical history, medicines, allergies, and adverse reactions immunisations, social history, family history and risk factors
- Medicare number (where available) for identification and claiming purposes
- healthcare identifier numbers
- health fund details.

Can you deal with us anonymously?

You can 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 is personal information collected?

We collect your personal information in several ways, depending on how you interact with the practice and the type of care you receive.

Direct collection from you

- When you make your first appointment, we collect your personal and demographic details through the patient registration process.
- Additional personal information is collected during the course of providing medical care.
- We may also collect information when you visit our website, send an email or SMS, call us, make an online appointment, or communicate with us through social media.

Collection through your healthcare interactions

We may collect further information through:

- electronic prescribing
- Safescript NSW
- My Health Record
- online appointment systems
- pathology, imaging, specialist, or hospital correspondence sent to us as part of your care

Collection from other sources

Where necessary for your care or required by law, we may receive personal information from:

- your guardian or responsible person
- other healthcare providers involved in your care, including specialists, allied health providers, hospitals, community health services, pathology and diagnostic imaging services
- Medicare, your private health insurer, or the Department of Veterans' Affairs (where relevant)

Collection of images and clinical photos

We may collect various forms of images as part of delivering healthcare and maintaining a safe environment.

CCTV footage

- CCTV is used on our premises for security and safety purposes in common areas of the practice (Hallways, waiting room, reception).
- Footage may incidentally capture patients, visitors, staff and contractors.

Clinical photos and medical images

- Clinical photographs may be taken during your care and form part of your health record.
- In some circumstances, these images may be taken using personal mobile devices. When this occurs, the practice follows RACGP guidance on the safe and appropriate use of personal devices for clinical photos.
- Images captured for clinical purposes are transferred promptly into your medical record and then securely deleted from the device used to capture them.
- Only the minimum necessary image is taken, and unnecessary background or identifying details are avoided where possible.
- We do not allow clinical photographs to be stored in personal galleries, cloud backups or messaging apps beyond the time required to securely transfer them into your record.

If you have concerns about the use of images during your care, please inform your clinician or the Practice Manager so we can discuss alternatives.

When, why and with whom we share your personal information

We may share your personal information when it is necessary for your healthcare, required by law, or needed to support safe and effective practice operations. We only disclose information to individuals or organisations that genuinely need it, and only to the extent required.

Sharing for healthcare and practice operations

We may share your personal information:

- with other healthcare providers involved in your care (for example in referral letters, reports, or shared care arrangements)
- through electronic prescribing and My Health Record (including Shared Health Summaries and Event Summaries)
- with third parties who support our business operations, such as accreditation bodies, information technology providers, and clinical or administrative service partners. These parties must comply with the Australian Privacy Principles and this policy.

Sharing when required or authorised by law

We may also share your information:

- when required or authorised by law, including responding to court subpoenas
- when necessary to lessen or prevent a serious threat to your life, health or safety, or to public health or safety, where it is impractical to obtain your consent
- to assist in locating a missing person
- to establish, exercise or defend an equitable claim
- as part of a confidential dispute resolution process
- when there is a statutory requirement to disclose certain information, such as mandatory notification of specific diseases

Overseas disclosure

We do not share your personal information with anyone outside Australia unless required or authorised by law, or unless you provide consent.

De-identified information

We may provide de-identified data to external organisations for quality improvement, training, or population health initiatives.

- This information does not identify individual patients.
- It is stored securely within Australia.
- We take steps to ensure the data cannot be re-identified.
- Patients may opt out of the use of their de-identified data at any time.

Direct marketing

We do not use your personal information for direct marketing without your express consent. If you choose to consent, you may opt out at any time by notifying the practice in writing.

Will your information be used for marketing purposes?

The practice does not use your personal information for direct marketing of goods or services without your express consent. If you choose to provide consent, you may withdraw it at any time by notifying the practice.

We may use your contact information to send messages that relate directly to your healthcare or the operation of the practice. These are not considered marketing under the Medical Board of Australia's advertising guidelines. Examples include:

- changes to billing policies or practice operations
- updates on clinician availability, relocations or extended leave
- clinically appropriate recalls and reminders
- evidence-based health promotion activities, such as screening and preventive care campaigns

These communications support continuity of care and are provided in line with AHPRA's expectations that information must be factual, responsible and not misleading.

For SMS messages, you can opt out at any time by replying **STOP**.
For emails, you may use the **unsubscribe** option included in our communications.

How is your information used to improve services?

The practice may use information to support safe, effective and continuously improving healthcare. We follow RACGP guidance on the primary and secondary use of general practice data and only use the minimum information necessary for these purposes.

Using personal information for internal quality improvement

We may use personal information within the practice to:

- monitor and improve the quality and safety of the services we provide
- conduct internal audits, reviews and analysis
- support training and development of the practice team

Only staff who require this information for these functions will have access to it.

Use of de-identified information

We may provide **de-identified** patient information to external organisations to support population health initiatives, quality improvement programs, reporting or training activities.

De-identified information, as defined by the RACGP, is information that has been altered or stripped of identifying details so that it no longer identifies an individual and is not reasonably likely to do so. Once information is appropriately de-identified, it is no longer considered personal information under the Privacy Act 1988.

If we share de-identified data:

- the information cannot identify individual patients
- it is stored securely and remains within Australia
- only the minimum necessary information is provided
- steps are taken to prevent re-identification

Patients may opt out of having their de-identified information included at any time by informing reception.

Identifiable data and research

Our practice does not currently participate in research that uses identifiable patient information. If this ever changes, we would seek your express, informed consent before releasing any identifiable information, and you would receive clear details about the project so you can decide whether or not to participate.

How are document automation technologies used?

The practice uses document automation technologies to streamline the creation of clinical documents, such as referral letters and care summaries. These systems draw on existing information in your medical record to generate documents efficiently and accurately.

Only information that is relevant to your care and necessary for the receiving healthcare provider is included. Templates are designed to limit unnecessary details and ensure patient privacy is protected.

These tools operate within our secure clinical software system (Best Practice). Each member of the practice team has a unique login and password and can only access information appropriate to their role.

All information processed through document automation is managed in accordance with Australian privacy legislation, the Australian Privacy Principles and the Royal Australian College of General Practitioners guidance on privacy and managing health information. Electronic and paper records are stored securely and handled in line with these requirements.

How are Artificial Intelligence (AI) Scribes used?

The practice uses AI-enabled tools to support clinical documentation, administrative workflows and appointment management. These tools assist our team but do not replace clinical judgement or decision-making. All AI systems used by the practice must comply with Australian privacy legislation, the Australian Privacy Principles and relevant RACGP guidance. We only use AI for purposes directly related to your care or essential practice operations.

AI scribe used during consultations (Heidi)

Some of our GPs use an AI scribe tool (Heidi) to help create clinical notes. The AI scribe works by generating a written summary from a real-time audio recording of your consultation. The GP reviews and approves the notes before they become part of your health record.

How Heidi is configured in our practice:

- The system records audio during the consultation solely to generate a clinical transcript.
- The audio recording is deleted immediately after transcription is complete.
- Heidi stores data only on secure Australian-based servers, in line with Australian Privacy Principles.
- Identifiable details in the transcript are automatically reduced or removed when appropriate.
- All notes generated by Heidi must be reviewed, edited and approved by your GP before they are added to your medical record.
- Heidi does not make clinical decisions and cannot override your GP's judgement.
- The AI scribe produces a draft summary only. Your GP reviews and approves the final note, and all clinical decisions are made exclusively by your doctor. AI outputs are used solely to support accurate documentation of your care.

Your choice:

You may opt out of the use of the AI scribe at any time. Inform your GP at the start of the consultation, and an alternative method of note taking will be used without affecting your care.

AI-assisted document processing (Samantha by CareGP)

The practice uses Samantha, an AI-assisted document processing tool, to support administrative tasks such as managing incoming pathology, imaging and specialist correspondence.

Samantha:

- reads and categorises incoming documents
- matches each document to the correct patient and GP
- imports material into Best Practice for clinician review
- is not autonomous — the practice team checks all documents prior to any clinical action
- does not make clinical decisions or modify clinical records independently

This tool reduces administrative workload and helps ensure documents reach the correct clinician promptly. Clinicians remain responsible for reviewing and acting on all correspondence.

AI-enabled phone assistant (Veronica)

The practice uses Veronica, a voice-enabled AI assistant, to help manage incoming phone calls. Veronica can assist with tasks such as booking and rescheduling appointments, sending reminders and providing basic practice information.

Call recording and transcription

To support accuracy, service quality and appointment management, calls handled by Veronica are recorded and transcribed.

- If your entire interaction is handled by Veronica, the **full call will be recorded and transcribed**.
- If you request to speak with a staff member at any time, **recording and transcription stop immediately**, and your call is transferred to reception.
- Recordings and transcripts are used only for operational purposes such as appointment management, quality improvement and system troubleshooting.
- All recordings are stored securely, retained only for the minimum period necessary and handled in line with Australian privacy law and the APPs.
- Veronica does not access your clinical record and does not make clinical decisions.

Your rights and our safeguards

- AI tools are used only for purposes directly related to your care or essential practice operations.
- AI systems do not provide diagnoses or clinical advice.
- You may opt out of the use of the AI scribe (Heidi) at any time.
- All AI outputs are reviewed by qualified staff.
- All data generated or handled by AI tools is managed in accordance with the Privacy Act, the APPs, and RACGP privacy guidance.
- The practice routinely reviews the security, accuracy and safety of all AI tools in use.

Real-time audio/visual recording, duplication, and storage of a consultation

The practice does not record consultations (including telehealth consultations) using audio or video. If this were to change in the future, recordings would only occur with your explicit, informed consent. Before any recording is made, we would explain the purpose, how the recording will be used, who can access it, how long it will be stored, and how it will be protected.

You would have the right to decline or withdraw consent at any time without any impact on your care. Any recordings would be handled with strict security measures and in full compliance with relevant privacy laws and professional standards.

How is your personal information stored and protected?

Your personal information may be stored in various forms, including:

- electronic medical records
- visual records such as X-rays, ultrasounds, CT scans, clinical photos or videos
- audio recordings created for clinical documentation or call management purposes
- administrative documents related to the provision of care

The practice stores all personal information securely, regardless of format.

Electronic information

Electronic records are stored within protected clinical information systems that use:

- strong password controls and unique user logins for all staff
- multi-factor authentication where available
- encryption of information in transit and at rest
- automatic system audit logs
- secure, regularly tested backup systems
- restricted access based on staff roles and responsibilities

Access to electronic records is limited to staff who require that information to perform their duties.

Paper and physical records

Paper documents are stored in secure areas of the practice with controlled access. These include locked cabinets, restricted administrative spaces and monitored records storage areas. Only authorised staff may access physical records.

Images, scans and clinical media

Visual records such as X-rays, CT scans, clinical photographs and other diagnostic images are stored securely within the relevant imaging platforms or linked medical record systems. When clinical photos are captured via mobile devices in line with practice policy, they are promptly transferred to the medical record and deleted from the device.

CCTV footage

The practice uses CCTV systems in certain non-clinical areas for security and safety. These areas may include external entry points, waiting rooms, hallways, and car park access points.

CCTV does **not** operate in consulting rooms, treatment rooms, or any area where clinical care is provided.
Footage is stored securely for a limited period, accessible only to authorised personnel, and may be released only where required or authorised by law.

AI-related recordings

Where AI tools such as the phone assistant (Veronica) record or transcribe calls, recordings are stored securely, retained only for the minimum time needed for quality assurance and operational purposes, and handled in accordance with Australian privacy law.

AI scribe audio recordings (Heidi) are deleted immediately once the transcription is complete.

Information governance and cybersecurity

We apply robust information governance and cybersecurity protocols, including:

- strict physical security procedures
- confidentiality agreements for all staff and contractors
- regular privacy and security training
- mandatory Privacy and Security Risk Assessments
- prompt action on any identified risks or incidents

These protections ensure that all personal information is managed safely, securely and responsibly.

How can you access and correct your personal information at the practice?

You have the right to request access to, or correction of, the personal information we hold about you.

Accessing your personal information

Patients may request access to their medical records at any time.
Please submit your request in writing to the Practice Manager. You can do this by email or by providing a written request at reception.

The practice will respond to your request **within 30 days**, in line with our internal processes and the Australian Privacy Principles.

In some cases, a reasonable fee may be charged to cover the administrative costs of providing access (for example, printing, preparing or transferring records). You will not be charged for making the request itself.

Correcting your personal information

The practice will take reasonable steps to ensure the information we hold about you is accurate, complete and up to date. We may ask you periodically to confirm your contact details and other key information.

If you believe any of your personal information is inaccurate or requires updating, please notify the practice so we can correct it. You may request updates by contacting the Practice Manager or advising our reception team.

We will respond to requests for correction promptly and will let you know the outcome.

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

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. We will then attempt to resolve it in accordance with our resolution procedure. The practice prohibits and actively monitors for any misuse of personal data, including doxxing, which is now recognised as a criminal offence under the Privacy Act.

Optimal Health Medical Centre Leppington	**Optimal Health Medical Centre Gregory Hills**	**Optimal Health Medical Centre Rhodes Central**
Shop C1.3c 108 Ingleburn Road Leppington, NSW, 2179	Suite 1, Unit 15a 1 Gregory Hills Drive Gledswood Hills, NSW, 2557	Shop 211a 6-14 Walker Street Rhodes, NSW, 2138
OR EMAIL: rebecca@ohmc.com.au		

You will be contacted within 30 days.

If you do not feel we have resolved your issue You may also contact the Office of the Australian Information Commissioner. The Office of the Australian Information Commissioner will require you to give them time to respond before they investigate. For further information visit **www.oaic.gov.au** or call the OAIC (Office of the Australian Information Commissioner) on 1300 363 992.

How is privacy on the website maintained?

We may collect personal information when you interact with the practice through our website, email, SMS, online appointment systems or social media.

Any personal information you provide through these digital platforms is handled securely and confidentially, in accordance with Australian privacy law and the Australian Privacy Principles.

Website analytics and cookies

Our website may use analytics tools and cookies to support site functionality, improve user experience and understand how people interact with our online services. These tools may collect information such as:

- device type
- browser type
- pages viewed
- time and date of visits
- general geographic location (not precise address)

This information is used only for operational and quality improvement purposes.
Cookies do not give us access to your clinical information or identify you directly unless you choose to submit your personal details through an online form.

Online forms and digital communication

If you choose to provide personal information via our website, email, SMS or social media (for example, when requesting an appointment), the information you provide will be used only for the purpose of responding to your enquiry or managing your care.

Security of online information

We take steps to protect information transmitted through digital channels, but no online system is completely risk-free. For this reason, we recommend you avoid including sensitive medical information in email or social media messages.

Policy review statement

The practice reviews this Privacy Policy regularly to ensure it remains accurate, compliant with current legal obligations and reflective of how we manage personal information.

We also conduct Privacy Impact Assessments (PIAs) before implementing any new technologies, systems or platforms that process personal health data or may pose higher privacy risks. This includes tools such as AI systems, telehealth platforms, automated document processing, wearable data integrations and other emerging technologies. These assessments help us understand and mitigate risks before introducing new services.

If the policy is updated:

- the most current version will always be available on our website
- significant changes that materially affect how your information is handled may be communicated directly to patients (for example, by email, SMS or clinic notices)

We encourage patients to check the policy periodically for updates.
If you have questions about this policy or how your information is managed, please contact the Practice Manager.