Gordonvale Family Medical Centre – Privacy Policy

Current as of: 13 May 2026

Introduction

This privacy policy explains how Gordonvale Family Medical Centre (GFMC) collects, uses, stores, protects and shares your personal information, including health information.

This policy is intended to comply with:

- The Privacy Act 1988 (Cth)
- The Australian Privacy Principles (APPs)
- Relevant Queensland health records and healthcare legislation
- RACGP Standards for General Practices
- Applicable digital health and cybersecurity obligations

This policy also outlines how our practice may use digital systems, including artificial intelligence (AI)-assisted technologies, to support healthcare delivery and business operations.

Why and when your consent is necessary

When you register as a patient of our practice, you provide consent for our doctors, nurses, allied health professionals and administrative staff to access and use your personal information so that we can provide healthcare services to you.

Only authorised team members who require access to your information in order to perform their duties will be permitted to access your records.

We will seek additional consent from you where:

- the use or disclosure is not directly related to your healthcare;
- sensitive information is proposed to be shared outside normal healthcare processes;
- recordings or images are proposed to be taken for education, training or other purposes;
- AI-assisted tools may be used in ways requiring additional patient awareness or consent.

You may withdraw consent at any time, subject to legal and clinical obligations.

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

Our practice collects personal information that is reasonably necessary to:

- provide medical care and treatment;
- manage your ongoing healthcare;
- communicate with you regarding appointments, recalls and reminders;
- process billing, Medicare and health fund claims;
- comply with legal and regulatory obligations;
- conduct accreditation, quality improvement and clinical audits;
- undertake staff education and training;
- maintain secure and effective business operations.

Information collected may include:

- your name, date of birth, address and contact details;
- Medicare, DVA and health fund details;
- medical history and family history;
- medications and allergies;
- investigation results and specialist correspondence;
- consultation notes and treatment records;
- digital communications and online booking information.

At your request and with your consent where required, information may also be shared electronically through systems including:

- My Health Record;
- electronic prescribing systems;
- the Australian Immunisation Register (AIR);
- secure messaging and referral platforms.

Definition of a patient health record

A patient health record is a comprehensive collection of information relating to your health, healthcare and treatment.

Complete and accurate records support continuity of care, patient safety and clinical decision-making.

Consultation records may include:

- date and time of consultation;
- clinician involved in the consultation;
- method of consultation (face-to-face, telephone, telehealth, email or electronic communication);
- presenting concerns and medical history;
- examination findings and investigation results;
- diagnoses and treatment plans;
- medications prescribed;
- referrals and specialist reports;
- allergies and adverse reactions;
- preventive healthcare information;
- consent documentation;
- communications relevant to your care.

Additional clinically relevant information may also be included where appropriate.

Dealing with us anonymously or under a pseudonym

Where lawful and practical, you may interact with our practice anonymously or using a pseudonym.

However, this may limit our ability to provide safe and effective healthcare services or comply with legal obligations.

Examples where anonymity may be possible include:

- providing general feedback;
- making non-clinical enquiries;
- participating in patient satisfaction surveys.

How do we collect your personal information?

We may collect your personal information:

- when you register as a patient;

- during consultations and treatment;
- through online bookings and patient portals;
- from telephone calls, emails, SMS or website communications;
- from referrals and correspondence from other healthcare providers;
- from hospitals, pathology and imaging providers;
- from Medicare, DVA or health insurers;
- through My Health Record and the AIR where authorised.

We currently use HotDoc and other secure digital systems to assist with appointment management and patient communications. Third-party providers engaged by the practice are expected to comply with Australian privacy obligations and maintain appropriate cybersecurity protections.

Any information you voluntarily publish publicly online, such as Google reviews or social media interactions, may be visible to the practice and the public.

GFMC does not routinely audio or video record consultations. If this changes in the future, specific patient consent would be obtained unless otherwise authorised by law.

Artificial Intelligence (AI) and digital technologies

GFMC may use approved digital technologies, including artificial intelligence (AI)-assisted systems, to support healthcare delivery, documentation, administration, quality improvement and operational efficiency.

Examples may include:

- clinical documentation support tools;
- medical transcription or summarisation systems;
- drafting referral letters or reports;
- appointment management and workflow systems;
- cybersecurity and fraud detection systems;
- population health or de-identified data analysis.

AI-assisted technologies are used as support tools only and do not replace the professional judgment of qualified healthcare practitioners.

Where AI-assisted systems are used:

- clinicians remain responsible for reviewing and approving clinical content;
- reasonable steps are taken to ensure information accuracy and patient safety;
- only authorised personnel may access patient information;

- systems are assessed for security, privacy and suitability;
- data handling practices are intended to comply with Australian privacy laws.

GFMC will not knowingly use identifiable patient information to train public AI models without appropriate consent or another lawful basis.

Where third-party AI or cloud-based providers are engaged, reasonable efforts will be made to ensure:

- contractual privacy and confidentiality protections exist;
- data is handled securely;
- information is stored within Australia where practicable, or otherwise protected in accordance with Australian privacy requirements.

Patients may request further information about the practice's use of digital or AI-assisted technologies.

When, why and with whom do we share your personal information?

We may share your personal information:

- with other healthcare providers involved in your care;
- with pathology, imaging and specialist providers;
- with Medicare, DVA and health insurers where required;
- with IT providers, accreditation agencies and contractors supporting practice operations;
- where required or authorised by law;
- where necessary to prevent or lessen a serious threat to life, health or safety;
- for mandatory public health reporting obligations;
- to support quality improvement and accreditation activities.

Only authorised persons requiring access to your information for legitimate healthcare or operational purposes will be permitted access.

We may provide de-identified or aggregated information to organisations such as Primary Health Networks for quality improvement, service planning or population health purposes. Patients may request exclusion from applicable data extraction programs where available.

Except where authorised or required by law, we will not disclose your personal information to third parties without your consent.

We will not disclose your personal information overseas without your consent unless:

- it is reasonably necessary for your healthcare;
- it is required by law; or
- appropriate privacy safeguards are in place.

Our practice does not sell patient information.

Sending your personal information

Your personal information may be securely transmitted outside the practice for healthcare and related purposes, including:

- specialist referrals;
- hospital referrals;
- pathology and imaging requests;
- insurer or solicitor requests authorised by you.

Where practicable, secure encrypted systems will be used, including:

- Medical Objects;
- Queensland Health Smart Referrals;
- Medicare secure messaging systems;
- encrypted email or password-protected documents.

Website, online services and cookies

Our website and online systems may collect limited technical information including:

- IP addresses;
- browser information;
- device information;
- website usage statistics.

This information may be used for:

- cybersecurity monitoring;
- website improvement;
- troubleshooting;
- analytics.

Our website may use cookies or similar technologies.

Third-party booking or communication providers may maintain separate privacy policies.

How do we store and protect your personal information?

GFMC stores personal information in secure electronic and limited physical formats.

Security measures include:

- role-based access controls;
- unique usernames and passwords for staff;
- multi-layered cybersecurity protections;
- firewall and network monitoring systems;
- audit logging and access monitoring;
- secure backups and disaster recovery systems;
- secure destruction or de-identification of information where appropriate.

Electronic records are stored on secure systems maintained by the practice and/or approved service providers.

While reasonable steps are taken to protect personal information, no electronic system can be guaranteed to be completely secure.

Staff receive training regarding privacy, confidentiality and cybersecurity obligations.

How can you access and correct your personal information?

You may request access to your medical records or request correction of inaccurate information.

Requests should be made in writing to:

Practice Manager
Gordonvale Family Medical Centre
11-15 Sicilian Avenue, Gordonvale QLD 4865
admin@gordonvalefamilymedical.com.au

We will respond within a reasonable timeframe, generally within 14 business days.

Administrative fees may apply for preparation or copying of records where permitted by law.

Access may be limited in certain circumstances permitted under the Privacy Act or other legislation.

How can you lodge a privacy complaint?

We take privacy concerns seriously.

If you have concerns regarding privacy, confidentiality or the handling of your personal information, please contact:

Practice Management
Phone: 07 4056 3600
Email: admin@gordonvalefamilymedical.com.au
Address: 11-15 Sicilian Avenue, Gordonvale QLD 4865

We will attempt to resolve complaints in accordance with our internal complaints process.

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

Office of the Australian Information Commissioner (OAIC)
Phone: 1300 363 992
Website: https://www.oaic.gov.au

Office of the Health Ombudsman (Queensland)
Phone: 133 646
Website: https://www.oho.qld.gov.au

Policy review statement

This privacy policy will be reviewed regularly and updated where necessary to reflect:

- changes to legislation;
- changes to RACGP standards;
- cybersecurity developments;
- changes to practice systems or technologies, including AI-assisted technologies.

The latest version of this policy will be made available:

- on our website;
- within the practice;

- upon patient request.

Disclaimer

This policy is intended as a general privacy policy for Gordonvale Family Medical Centre.

It does not constitute legal advice.

The practice may seek independent legal, privacy, cybersecurity or regulatory advice to ensure ongoing compliance with applicable laws and professional standards.