



Privacy Policy

Policy Owner	Practice Manager	Version	5.0
Effective Date	August 2026	Next Review	August 2027
Approved By	Practice Principal / Practice Management	Status	Current

1. Purpose

This Privacy Policy explains how Glenmount Medical Clinic collects, holds, uses, discloses, stores and protects personal information, including health information. It also explains how patients can access and request correction of their information, how privacy concerns are managed, and how patients can contact the practice about privacy.

The policy is written for patients and is intended to support the practice's obligations under applicable privacy laws and the RACGP Standards for general practices, 5th edition.

2. Our commitment to privacy

- We only collect information that is reasonably necessary for providing healthcare and related practice functions.
- Access to patient information is limited to team members who need it for their role.
- We use reasonable safeguards to protect information against misuse, loss, unauthorised access, modification or disclosure.
- We will explain, where appropriate, why information is collected and how it may be used or disclosed.
- We will not use health information for direct marketing unless the patient has given express consent.
- We will respond to privacy concerns and complaints and use them as opportunities for quality improvement.

3. What personal information do we collect?

Depending on the services provided and the patient's circumstances, we may collect:

- name, date of birth, address and contact details;
- emergency contact and relevant demographic information;
- medical history, diagnoses, medications, allergies, adverse reactions, immunisations, family history, social history and risk factors;
- clinical notes, observations, photographs where clinically appropriate, correspondence, referrals, reports, investigations and test results;
- Medicare details, healthcare identifiers and health fund information where relevant;
- billing and payment information;
- information provided by authorised representatives, carers or guardians; and
- information relevant to the safe and effective provision of healthcare.





4. What is a patient health record?

A patient health record is information about a patient held in paper or electronic form. It may include demographic and contact information, medical history, treatment notes, observations, correspondence, investigations, test results, photographs, prescriptions, medication records, reports and other information relevant to the patient's care.

5. How do we collect personal information?

Information may be collected directly from the patient or, where appropriate, from other sources. This may occur when:

1. a patient registers with the practice or makes an appointment;
2. a patient attends a consultation or receives treatment;
3. a patient contacts the practice by telephone, email, SMS or another approved communication method;
4. a patient uses the practice website or online appointment service such as HotDoc;
5. information is received from other healthcare providers, including specialists, allied health professionals, hospitals, pathology providers and diagnostic imaging services;
6. information is received from Medicare, the Department of Veterans' Affairs or a health fund where necessary; or
7. information is obtained from an authorised guardian, responsible person or carer where appropriate.

6. Why do we collect, use and hold personal information?

The main purpose is to provide safe, effective and coordinated healthcare. We may also use information for directly related practice activities, including billing and claims, recalls and follow-up, quality improvement, accreditation, audit, staff education and training, and practice administration.

Where the practice uses approved clinical or documentation-support technologies, only information necessary for the relevant purpose is used. The practice will follow applicable consent, privacy and security requirements for these systems.

7. Electronic health services and communication

Glenmount Medical Clinic participates in electronic health services including electronic transfer of prescriptions (eTP), My Health Record and electronic referral systems such as HealthLink where applicable. The practice may also use online appointment and communication services such as HotDoc.

Patients should be aware that electronic communication, including email and SMS, has privacy and security risks. The practice will take reasonable steps to use approved systems, verify recipient details and minimise unnecessary sensitive information in electronic messages. Email and SMS are not monitored continuously and must not be used for emergencies.

Real-time audio or visual recording, duplication or storage of consultations, including telehealth consultations, will not occur without appropriate patient consent.





8. Consent

When a patient registers with the practice, consent is generally obtained for the practice team to collect, access, use and disclose information as reasonably necessary to provide healthcare and manage the patient's care.

Where information is proposed to be used or disclosed for another purpose that is not reasonably expected or otherwise authorised by law, additional consent will be sought where required.

Patients may withdraw consent where withdrawal is legally and clinically practicable. Withdrawal of consent may affect the practice's ability to provide certain services.

9. Use and disclosure of personal information

We may disclose personal information when it is necessary to provide healthcare, for purposes reasonably expected by the patient, with the patient's consent, or where permitted or required by law. This may include disclosure to:

- other healthcare providers involved in the patient's care;
- hospitals, pathology and diagnostic imaging services;
- allied health professionals and other relevant care providers;
- Medicare, the Department of Veterans' Affairs or health funds where required for relevant services or claims;
- service providers supporting the practice's systems, technology, accreditation or business functions, where appropriate safeguards are in place; and
- government or regulatory bodies where disclosure is required or authorised by law.

Information may also be disclosed where necessary to lessen or prevent a serious threat to a person's life, health or safety or public health or safety, where legally permitted, or for other permitted situations under applicable privacy law.

10. Overseas disclosure

Glenmount Medical Clinic will not knowingly disclose personal information overseas unless the disclosure is authorised or permitted under applicable privacy law and appropriate safeguards are in place. Where required, the practice will take reasonable steps to ensure the overseas recipient handles the information consistently with applicable privacy requirements.

11. Direct marketing

The practice will not use health information for direct marketing unless the patient has expressly consented. Where a patient has consented to receive direct marketing, they may opt out at any time by contacting the practice.

12. Anonymity and pseudonyms





Patients may generally deal with the practice anonymously or using a pseudonym where it is lawful and practicable to do so. This may not be possible where identification is necessary to provide safe healthcare, to verify a patient's identity, to process a Medicare or other claim, or where the law requires the practice to identify the individual.

13. How we store and protect information

Patient information is stored in electronic and, where applicable, paper records. The practice uses access controls, passwords and other reasonable security measures to protect information. Access is limited according to staff roles and responsibilities.

The practice maintains appropriate backup arrangements and takes reasonable steps to ensure information can be restored when required. Staff and contractors are required to maintain confidentiality and comply with the practice's information security and privacy requirements.

Information will be retained and securely disposed of in accordance with applicable Victorian and Commonwealth requirements and the practice's records management procedures. Retention periods may vary depending on the type of record and the age of the patient.

14. Access to personal and health information

Patients have a right to request access to personal and health information held by the practice, subject to limited exceptions under applicable law.

A patient may contact reception or the Practice Manager to request access. The practice may ask for information to verify identity and may ask the patient to put the request in writing to assist with processing it. Patients may request access in a particular form, although an alternative form may be used where the requested method is unreasonable or impracticable.

The practice aims to respond to access requests within 30 days. If access is refused, the practice will provide written reasons where required and information about available complaint mechanisms.

Reasonable fees may apply for providing copies or other services where permitted by Victorian law. The practice will advise the patient of any applicable fee before proceeding where practicable.

15. Correction of personal and health information

Patients may ask the practice to correct personal or health information that is inaccurate, incomplete, out of date, irrelevant or misleading. Requests may be made verbally or in writing; the practice may ask for written confirmation to assist with processing.

The practice will take reasonable steps to correct information where appropriate and will generally respond to a correction request within 30 days. There is no charge for making a correction request, correcting information or associating a statement with information where required by privacy law.

If the practice refuses a correction request, the patient will be informed of the reasons where required and advised of available complaint options.





16. Transfer of medical records

Patients who wish to transfer their medical records to another healthcare provider may request this through reception or the Practice Manager. The practice will follow its records transfer procedure and applicable privacy requirements. Any permitted administrative or copying fees will be advised before they are incurred.

17. Privacy complaints

Patients who have a privacy concern or complaint may raise it with their treating doctor, reception team or Practice Manager, verbally or in writing. The practice will acknowledge and investigate the concern, take reasonable steps to resolve it, and provide information about external complaint options where appropriate.

Privacy complaints should be managed in accordance with the practice's Complaints and Feedback Policy and Privacy Breach/Incident Management procedures. Where a privacy breach occurs, the practice will assess and respond in accordance with applicable privacy law, including the Notifiable Data Breaches scheme where applicable.

18. External privacy complaints

If a patient is not satisfied with the practice's response, they may contact the Office of the Australian Information Commissioner (OAIC) for privacy complaints. Victorian health privacy complaints may also be made to the Health Complaints Commissioner (HCC).

OAIC: www.oaic.gov.au | 1300 363 992

Health Complaints Commissioner Victoria: www.hcc.vic.gov.au | 1300 582 113

19. Privacy and children / authorised representatives

The practice recognises that privacy and access arrangements may differ for children and for people who have an authorised guardian, substitute decision-maker or other representative. The practice will verify authority and apply the requirements of applicable law when deciding whether information can be accessed or disclosed to another person.

20. Privacy and third-party services

Where the practice uses external providers for technology, appointment booking, information management, accreditation, document support or other business functions, the practice will take reasonable steps to ensure that patient information is handled appropriately and securely and in accordance with applicable privacy obligations.

21. Staff confidentiality and access

Only team members who require access to patient information for their role should access that information. Staff must not access records out of curiosity or for purposes unrelated to their role. Staff and





Glenmount
Medical Clinic
ESTABLISHED 1958

*Your Health
Our Priority*

contractors are required to comply with confidentiality, privacy and information security requirements and may be subject to disciplinary action where these requirements are breached.

22. Policy review and availability

A copy of this Privacy Policy is available to patients on request and will be made available through the practice website where applicable. The policy will be reviewed at least annually and sooner where there are significant changes to legislation, practice systems, services or privacy risks.

Patients will be notified of significant changes where reasonably practicable.



598 High Street Road,
Glen Waverley VIC 3150



03 9802 9101



03 5296 5818



info@glenmountmedical.com
www.glenmountmedical.com