177 Burke Road
Glen Iris, Vic, 3146
Ph: 03 9509 7633
Fax: 03 9509 6177
www.glenirismg.com.au

Privacy Policy

About this Policy

This policy was updated on 30th October 2024.

Glen Iris Medical Group ("us", "we", or "our") recognises the importance of your privacy and respects your right to control how your personal information is collected and used. We are committed to protecting the privacy of patient information and to handling your personal information in a responsible manner.

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. This policy is aligned with the Australian Privacy Principles (APP) as set out in the Privacy Act 1988 (Cth) (Privacy Act) and describes the way that we may collect, hold and disclose personal information. We are an APP Entity as defined in the Privacy Act 1988 (Cth) (the "Act").

This privacy policy applies to our website, www.glenirismg.com.au (the "Site") which is operated by us, and to the products and services provided by us.

In this policy, "personal information" means any information that may identify you, or by which your identity might be reasonably determined. The information you provide us may include, amongst other things, your name, address, and contact details.

"Sensitive Information" means any information about an individual's racial or ethnic origin, political opinions, religious belief or affiliation, philosophical belief, membership of a professional or trade association, membership of a trade union, sexual preference or practices, criminal record or health information.

A patient's "medical record" or "health information" is any personal information about you and your illness, injury or disability.

Some examples of health information include:

- Clinical notes regarding your symptoms or diagnosis
- Information about services you've had or will receive
- Specialist reports and test results
- Prescriptions and other pharmaceutical purchases
- Your wishes about future health care or organ donation
- Appointment and billing details
- Any other personal information about you that is collected by a health service provider

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 or doctors 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.

Collection

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/payments, practice audits and accreditation, or business processes (eg. staff training).

We may collect personal Information such as:

- Your name, date of birth, address and contact details
- Your payment and billing information
- Medical information including medical history, medications, allergies, immunisations, family history and risk factors
- Medicare and concession card numbers
- Details of conversations we have had with you or any other information relevant to us

We automatically collect through our Site and services, additional information that is often not personally identifiable, such as the website from which visitors came to our Site, IP address, browser type and other information relating to the device through which they access the Site. We may combine this information with the personal information we have collected about clients.

We may collect your information in several different ways:

1. When booking your first appointment with our practice we will collect personal and demographic information via your registration.

2. During the provision of medical services including through electronic transfer of prescriptions (eTP), My Health Record and other eHealth services.

3. We may collect personal information when you visit our website, send us an email or SMS, phone us, make an online appointment, use the AMS Connect app or communicate with us via social media.

4. In some circumstances personal information may 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 parent, guardian or responsible person
   - other healthcare providers, such as specialists, allied health, hospitals, pathology or diagnostic imaging services
   - Medicare, or the Department of Veterans' Affairs

We will always comply with privacy obligations when collecting personal information from third-party sources. This includes obtaining necessary consents and transparency with patients.

Various types of images may be collected, including CCTV footage for safety and security purposes (waiting room, reception, hallway and front entrance areas only) and photos/medical images taken for medical purposes. Real-time audio/visual recording of a consultation, including those via telehealth, will never occur without patient consent.

Anonymity & Pseudonymity

APP entities must give individuals the option of not identifying themselves or using a pseudonym, unless it is impractical to do so or unless required or authorized by law to only deal with identified individuals.

Patients should be aware that there may be consequences if they do not identify themselves, such as for their ongoing healthcare and ability to claim a Medicare or health fund rebate.

Use & Disclosure

Personal information collected by us will generally only be used and disclosed for the purpose it was collected.

We may from time to time use personal information for another purpose where it would be reasonably expected by you or if permitted by the Privacy Act, including to effectuate or enforce a transaction, procuring advice from legal or accounting firms, auditors and other consultants.

We may also use and share aggregate or non-personally identifying information about clients for market analysis, research, marketing, to improve the quality of our services or other purposes.

We sometimes share your personal information:
- With third-parties who work with us for business purposes, such as accreditation agencies or IT 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
- When it is necessary to lessen or prevent a serious threat to a patient's life, health or safety, or public health or safety, and 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 confidential dispute resolution process
- When there is a statutory requirement to share certain personal information (eg. some diseases require mandatory notification)
- During the provision of medical services, through eTP or My Health Record

Other than in the course of providing medical services or as described in this policy, our practice will not share personal information with any third-party without your consent. We do not provide your personal information to other organisations for the purposes of direct marketing.

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. Please let reception know if you do not want your information included.

Our practice uses referral templates that extract your personal information into referral letters through document automation technologies, particularly so that only the relevant medical information is included in referral letters. This technology is used through secure medical software Best Practice. All users of this software have their own unique user credentials and passwords and can only access information that is relevant to their role in the practice team.

In addition, we may electronically send relevant information to service providers via secure messaging systems.

Storage & Security

Your personal information may be stored at our practice in various forms but primarily in the form of electronic patient records. We may also store your information in the form of paper records or visual records (eg. X-ray images and photos).

We will take reasonable steps to protect your personal information from misuse, loss, unauthorised access and modification or disclosure. We use commercially reasonable physical, technical and administrative measures to protect personal information that we hold, including, where appropriate, password protection, encryption, and SSL to protect our Site. All staff and contractors sign confidentiality agreements before commencing at the practice.

Despite taking appropriate measures to protect personal information used and collected by us, please be aware that no data security measures can guarantee 100% security all of the time. We cannot guarantee the security of any information transmitted to us via the internet and such transmission is at your risk.

If we no longer require your personal information, we will take reasonable steps to destroy or permanently de-identify it.

Personal information may be stored electronically through third-party data centres, which may be located overseas, or in physical storage at our premises or third-party secure storage facilities.

You are solely responsible for the maintaining the secrecy of any passwords and other account information pertaining to our Site, app or services.

Please refer to the statement on Cyber Security from our IT partner Digital Medical Systems (DMS) for further information. This can be obtained from reception or via our website.

Access & Accuracy

You can access and/or correct information we hold about you at any time by contacting the Practice Manager. We encourage you to keep your personal information 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.

We will respond to your request for personal information within 30 days. We may charge an administration fee to cover the costs of responding to your request (eg. for retrieving information from storage, or if photocopies need to be made).

We require a consent form signed by you for medical record transfers to another practice before we will provide them with a copy of your medical record. A transfer fee may apply to cover associated administration costs.

If you request for your personal health information to be emailed to you, you will first be asked to review and consent to a document advising that email transmissions are not secure.

If required by law or where the information may relate to existing or anticipated legal proceedings, we may deny your request for access to your information. We will respond to your request, explaining the reasons for refusal in writing.

Cookies, Web Beacons & Analytics

When you interact with our Site, we, or our third-party service providers, may use cookies, web beacons (clear GIFs, web bugs) or similar technologies to track site visitor activity or collect site data. We may combine this data with the personal information we have collected.

Examples of information that we may collect include technical information such as IP address and browser type, and information about your visit such as the products viewed or searched for, the country you are in, what you clicked on and what links you visited to get to or from our site.

If we identify you with this information, any use or disclosure of that information will be in accordance with this privacy policy.

Third-Party Websites

At times, our Site may contain links to third-party websites. Any access to and use of such websites is not governed by this privacy policy, but is instead governed by the privacy policies of those third-party websites. We are not responsible for the information practices of such third-party websites.

Career Applications

Employment applications and resumes collected by us are safely and securely stored and only used for the purposes for which they were collected.

International Transfer

We may transfer your personal information to organisations in other countries. Recipients may include our related entities or employees, external service providers such as administration providers or IT providers such as cloud storage and data processing. We only transfer information where we reasonably believe that the recipient is legally or contractually bound to principles that are very similar to the Australian Privacy Principles.

Marketing Emails

We may send you direct marketing emails and information about products and services that we consider may be of interest to you. These communications will only be sent via email and in accordance with applicable marketing laws, such as the Spam Act 2004 (Cth) as per your consent upon registering for our services.

If you would like to stop receiving these promotional emails, you may follow the opt-out instructions contained in any such email. It may take up to 10 business days for us to process opt-out requests. If you opt-out of receiving emails or promotions from us, we still may send you email about your account, any services you have requested or received from us, or for other customer service purposes.

Data Breach Notification Scheme

If we suspect a data breach has occurred, we will undertake an assessment in accordance with the Notifiable Data Breach Scheme. If we determine there has been an eligible data breach, we will notify you as soon as reasonably practicable.

If the breach relates to the My Health Records Act, we may disclose your personal information to the My Health Records System Operator under s 73A of that Act.

Changes to this Policy

This privacy policy will be reviewed annually or as required and we may make changes as needed. Updated versions of this privacy policy will be made available at reception and posted on our Site. You should check periodically to review our current privacy policy, which is effective as of the effective date listed.

Your continued use of any of our Site and services constitutes your acceptance and understanding of the privacy policy as in effect at the time of your use. If we make any changes to this privacy policy that materially affect our practices with regard to the personal information we have previously collected from you, we will endeavour to provide you with notice in advance of such change by highlighting the change on the Site, or where practical, by email.

Complaints & Enquiries

We take complaints and concerns regarding privacy seriously. If you have any questions or complaints regarding privacy or this policy, or if at any time you believe we may have wrongfully disclosed your Personal Information or breached this privacy policy, please contact our Practice Manager via the details below and we will respond within 30 days:

Practice Manager
Glen Iris Medical Group
177 Burke Road
Glen Iris, Vic, 3146

Ph: 03 9509 7633
admin@glenirismg.com.au

If you are not satisfied with our response, you are entitled to lodge a complaint with:

Office of the Australian Information Commissioner
GPO Box 5288
Sydney, NSW, 2001

Ph: 1300 363 992
Fax: 02 6123 5145
www.oaic.gov.au