

Privacy Policy

1. INTRODUCTION

- 1.1 This Privacy Policy is to provide information to you on how your personal information (which includes your sensitive information, including your health information) is collected and used within our practice, Mt Martha Village Clinic, and the circumstances in which we may share it with third parties.

2. HOW AND WHY YOUR CONSENT IS NECESSARY

- 2.1 When you register as a patient of a practitioner who consults from our practice, you provide consent for us (including our employees, agents, contractors and other representatives) to access and use your personal information so the independent practitioners consulting from our practice can provide you with the best possible healthcare. Only persons who need to see your personal information will have access to it. If we need to use your information for any other purposes, we will seek additional consent from you to do so.

3. WHY DO WE COLLECT, USE, HOLD AND SHARE YOUR PERSONAL INFORMATION

- 3.1 Our practice will need to collect your personal information to facilitate the provision of healthcare services to you by the independent practitioners consulting from our practice. Our main purpose for collecting, using, holding and sharing your personal information is to facilitate the management of your health by those independent practitioners. We also use it for directly related business activities such as financial claims and payments, practice audits and accreditation, and business processes (for example: staff training).

4. WHAT PERSONAL INFORMATION DO WE COLLECT

- 4.1 The information we will collect about you includes your:
- (a) Names, date of birth, address, contact details including emergency contact and next of kin;
 - (b) Demographic information, including birth sex, gender identity, cultural background, occupation and religious beliefs;
 - (c) Medical information including medical history, medications, allergies, adverse events, immunisations, social history, family history and risk factors;
 - (d) Medicare and Department of Veterans Affairs' number (where available) for identification and claiming purposes.
 - (e) Healthcare identifiers

- (f) Concession card details; and
- (g) Health fund details

5. DEALING WITH US ANONYMOUSLY

- 5.1 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.
- 5.2 Please be aware that Medicare rebates are only available where a Medicare card (and / or associated information) is available. As such your practitioner may require you to pay for your consults in full without this rebate if you choose to deal with us anonymously or under a pseudonym.

6. HOW DO WE COLLECT YOUR PERSONAL INFORMATION

- 6.1 Our practice may collect your personal information in several different ways:
 - (a) You may provide us with your personal information directly (for example, when you make an appointment with a practitioner consulting from our practice, our practice staff will collect your personal information via your registration);
 - (b) The independent practitioners providing medical services may also collect further personal information from you which may be disclosed to us. Information can also be collected through My Health Record for example via Shared Health Summary, Event Summary or through Discharge Summary provided by a hospital or other healthcare service providers;
 - (c) We may also collect your personal information when you contact us via our website, send us an email or SMS, telephone us, make an online appointment or communicate with us using social media, and;
 - (d) 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:
 - i your guardian or responsible person
 - ii other involved healthcare providers, such as specialists, allied health professionals, hospitals, community health services and pathology and diagnostic imaging services; and / or
 - iii your health fund, Medicare, or Department of Veterans' Affairs (as necessary)
- 6.2 If your practitioner deems it in your best interest to discuss your clinical information with you, we will arrange for this to occur either in person, via telephone or via videoconference.

7. WHEN, WHY AND WITH WHOM DO WE USE AND SHARE YOUR PERSONAL INFORMATION

- 7.1 We collect, use and disclose your personal information to facilitate the provision of medical services to patients of the independent practitioners consulting from our practice.
- 7.2 We may use your personal information:
- (a) With other healthcare providers.
 - (b) When it is required or authorised by law (for example court subpoenas, or where we are obliged to make a mandatory notification to a regulatory body).
 - (c) 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 where it is otherwise impractical to obtain your consent.
 - (d) To assist in locating a missing person.
 - (e) To establish, exercise or defend a claim
 - (f) For the purposes of confidential dispute resolution processes
 - (g) During the course of providing nursing support services
 - (h) For the purposes of uploading that information to your My Health Record, such as through the Shared Health Summary or Event Summary.
 - (i) 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 the Australian Privacy Principles (APPs) and this policy.
 - (j) Where your practitioner will be obliged to release personal health information without your express consent such as in treating a serious threat to your life, health and safety or if it is impracticable to obtain your consent.
 - (k) Where de-identified information may be used for research and quality assurance activities and professional development to improve individual and community health. Your practitioner uses software (named POLAR) that reports de-identified data to secure health services to improve planning in this area.
- 7.3 Only people who need to access your information will be able to do so. Other than in the course of facilitating the provision of medical services or as otherwise described in this policy, our practice will not share personal information with any third party without your consent.
- 7.4 We will not share your personal information with anyone outside Australia (unless under exceptional circumstances that are permitted by law) without your consent.

- 7.5 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 not consent, you may opt out of direct marketing at any time by notifying our practice in writing.
- 7.6 We may provide de-identified data to other organisations to improve population health outcomes. You can let our reception staff know if you do not want your de-identified data included.
- 7.7 Your practitioner may use artificial intelligence to record and summarise your consultation and store the transcript of the appointment in your medical record. These notes will be reviewed by your practitioner to ensure they accurately reflect your appointment before they are relied upon to provide medical service.
- 7.8 We cannot and do not, determine or instruct the independent medical practitioners about how they deliver their medical services to you, including which artificial intelligence program they utilise for their patient consults. We therefore cannot make any warranties or guarantees on how specific artificial intelligence programs will collect, store or use data. Please direct any queries or concerns you have in relation to the artificial intelligence program directly to your practitioner. They will also provide you with access to the relevant terms and conditions and privacy policy for the specific artificial intelligence program they use. We will not be liable under any circumstances for any damages of any kind recognised by law due to artificial intelligence program and liability is limited to the extent of our negligence or misconduct. We will participate in updating you on your practitioner's behalf if needs be of any communications received you're your practitioners in relation to the artificial intelligence program. Any complaints should be sent directly to the owner of the artificial intelligence program.

8. HOW DO WE STORE AND PROTECT YOUR INFORMATION

- 8.1 Your personal information may be stored at our practice in various forms
- 8.2 Our practice stores information as electronic records (including via cloud-based services), paper records and visual records (including X-rays, CT scans, videos and photos).
- 8.3 Our practice is monitored with an alarm system and stores all personal information securely via the use of passwords, 2-step authentication (in certain circumstances), different levels of staff access depending on role, encrypted back-ups, confidentiality agreements for staff and secure cabinets.
- 8.4 All records will be retained until the later of seven (7) years for your last contact with the practice, or until you reach the age of twenty-five (25).

- 8.5 We take steps to destroy or de-identify information that we no longer require.
- 8.6 Our server security policy is designed to protect the services 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) Public facing servers are placed on their own subnet and workstations and internal servers are 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 are installed around the building.
 - (f) Servers are patched regularly to fix the security vulnerabilities
 - (g) Backups are created regularly every hour onsite with daily offsite backups.

9. HOW CAN YOU ACCESS AND CORRECT YOUR PERSONAL INFORMATION AT OUR PRACTICE

- 9.1 You have the right to request access to, and correction of, your personal information.
- 9.2 Our practice acknowledges patients may request access to their medical records. You can lodge an initial request via email or telephone. Our practice will acknowledge your request within three (3) business days and send you a pro forma to complete and lodge. 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 reasonable costs incurred in complying with your request.
- 9.3 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 confidential@mmvc.com.au. There is no fee charged for making corrections to your personal information.

10. HOW CAN YOU LODGE A PRIVACY-RELATED COMPLAINT, AND HOW WILL THE COMPLAINT BE HANDLED AT OUR PRACTICE

- 10.1 We take complaints and concerns regarding privacy seriously. You should express any privacy concerns (including any breach of the APPs or any registered binding APP code) you have in writing.

- 10.2 Complaints should be addressed to:
- (a) Name and Position: The Practice Manager
 - (b) Address: Mt Martha Village Clinic, 2 Langrigg Avenue, MT MARTHA VIC 3934
 - (c) Email: confidential@mmvc.com.au
- 10.3 We will respond with acknowledgement of your complaint within three (3) business days and provide a response within thirty (30) business days.
- 10.4 You may 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 or call the OAIC on 1300 363 992.
- 10.5 You may also contact the Office of Victoria Information Commissioner (OVIC). For further information, visit ovic.vic.gov.au or call the OVIC on 1300 006 842

11.WEBSITE COOKIES AND TRACKING TECHNOLOGIES

- 11.1 If you “like” or comment on our social media pages, we will have your social media name.
- 11.2 Our website uses cookies to enhance your browsing experience. A “cookie” is a small text file stored in your browser, which helps manage website settings and deliver relevant content. We may collect non-identifiable information such as your device type, browser type, IP address and the pages you visit on our website and certain third-party websites. This information does not personally identify you. You can manage how your browser handles cookies by adjusting your browser settings. Please note that disabling cookies may limit your ability to access certain features or content on our website.
- 11.3 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.

12.PRIVACY STATEMENT REVIEW

- 12.1 This privacy policy will be reviewed annually to ensure it is in accordance with any changes that may occur.
- 12.2 Last reviewed 19 June 2025.