DR ROBARTS VETERAN CONSULTANCY PRIVACY POLICY – V3.2

INTRODUCTION & OVERVIEW

Here at Renee Michelle Robarts ABN 33 682 939 458 trading as Dr Renee Robarts Veteran Consultancy (**we**, **us** or **our**) protecting your privacy and treating your personal data in accordance with Australian privacy laws with care is of paramount importance to us. This Privacy Policy also applies to our related bodies corporate.

This Privacy Policy explains what personal data we collect, why we collect personal data and how we collect, use, disclose, store and protect your personal data when you visit our website, use our services or products, provide us with information yourself (such as when you sign up to our service or use our services) or when you accept services from us. We collect and process your personal data for specific purposes including: to provide and improve our services, to communicate with you, to personalise your experience, to enable third parties to be engaged by us to provide services to you on your behalf, for analytics and research, and to comply with legal obligations.

It also explains how to contact us to correct, update or delete any personal data provided to us, or make a complaint if you have concerns.

We are compliant with the *Privacy Act 1988* (Cth) (**the Act**) and the Australian Privacy Principles (**APPs**). In the event of a data breach, we have a clear and actionable response plan in place. This includes promptly notifying affected individuals and relevant authorities, containing the breach, assessing its impact, and implementing measures to prevent future occurrences. If you have any questions or concerns about our data handling practices, please contact our Privacy Officer at contact@drvc.com.au.

We will only collect and process personal data about you where we have a lawful basis to do so. Lawful basis includes consent (where you have given consent), contract (where processing is necessary for the performance of a contract with you), legal obligation (where processing is necessary for compliance with a legal obligation we have), and legitimate interests (including security threats or fraud, risk of harm to self or others, compliance with applicable laws, and enabling us to administer our service).

If you choose to withdraw your consent, we will stop processing your personal data for the purposes you initially agreed to, unless we have another lawful basis for doing so. This may result in limited access to certain features or services that require the processing of your personal data. We will retain your data only as necessary to comply with legal obligations or resolve disputes.

We maintain secure records of all user consents and withdrawals to ensure compliance with data protection regulations and to respect your privacy choices. These records are kept for the duration of our relationship with you and for a reasonable period thereafter as required by applicable laws.

Unless otherwise indicated by the context words importing the singular include the plural and vice versa and references to *personal information* includes a reference to *Sensitive Data* described below.

CHANGES THAT WE MAKE TO OUR PRIVACY POLICY

We will notify you about any changes to our Privacy Policy by updating the “Last Updated” date of this Privacy Policy. You are encouraged to periodically review this Privacy Policy to stay informed of updates. We will seek your explicit consent for any changes in our Privacy Policy that affect how we process your personal data. If you do not agree with the changes, you may choose to stop using our services.

COLLECTION OF YOUR PERSONAL DATA BY THIRD PARTIES

This Privacy Policy does not apply to any third-party service we engage to provide services to us for you or website which we connect to, and which may also collect and use information about you. We are not responsible for the privacy practices of any third party. However, we take reasonable steps to ensure that third parties who are required to access your personal information as part of the services we provide to you have at least the same level of security we employ to protect your personal information.

IF YOU DO NOT AGREE WITH THE TERMS OF THIS PRIVACY POLICY, PLEASE DO NOT ACCESS OUR WEBSITE, USE OUR SERVICES OR PROVIDE ANY INFORMATION ABOUT YOURSELF TO US.

WHICH ENTITIES DOES THIS PRIVACY POLICY COVER?

This Privacy Policy applies to us with respect to content on our websites, our services and information you provide to us about yourself.

WHAT IS PERSONAL DATA?

Personal data is defined as data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access. Personal data may include sensitive information such as health information about you.

WHEN AND HOW DO WE COLLECT YOUR PERSONAL DATA?

We collect most personal data directly from you when you consent to use our services or receive communications from us, or information we receive from third parties. Your consent may be express (e.g. you agree to the use of your information by ticking a box) or implied by an action you take or do not take (i.e. because you have agreed to terms and conditions that contain information about the use or disclosure of your information).

We will collect personal information:

- from you directly when you provide your details to us. This might be via a face-to-face discussion, telehealth consultation, telephone conversation, registration form or online form;
- from a person responsible for you; or
- from third parties where the Act or other law allows it which may include, but is not limited to other members of your health care team, diagnostic centres, specialists, hospitals.

You provide us your information when you use our products, services or you use our website generally or you deal with us.

WHAT PERSONAL DATA DO WE COLLECT?

We may collect and process various types of personal data, including sensitive personal data. Under the Act, sensitive personal data includes information such as racial or ethnic origin, political opinions, religious beliefs, health information (**Sensitive Data**). When we collect Sensitive Data, we implement additional safeguards to protect this information, including enhanced security measures, stricter access controls, and specialised handling procedures in compliance with applicable laws and regulations**.**

We collect personally identifiable information either directly from you or as provided to us through third parties that you have consented to disclose such information. That personally identifiable information, collected in compliance with the Act, may include (but not be limited to):

- full name;
- mailing or street address;
- date of birth;
- email address;
- telephone number and other contact details;
- age or date of birth;

- occupation;
- DVA number and related details;
- sensitive health information from your third party healthcare team including medical records, medical reports, test results, diagnostic and imaging reports;
- your device ID, browser type and version, device type, geo-location information, computer and connection information, statistics on page views, traffic to and from the sites, IP address and standard web log information;
- details of the services we have provided to you or that you have enquired about, including any additional information necessary to deliver those services and respond to your enquiries;
- any additional information relating to you that you provide to us directly through our website or via email or use of our services or indirectly through your use of our website or use of our services or online presence or through other websites or accounts from which you permit us to collect information;
- information you provide about yourself when you communicate to us or others when you use the services;
- information you provide to us through our information request processes including our online forms; or
- any other personal data that is directly related to and necessary for facilitating your dealings with us, as explicitly stated at the time of collection.

We may collect these types of personal data either directly from you, or from third parties or from third party applications you control and give us access to. We may collect this information when you:

- register for our products or services; and
- communicate with us through correspondence or email;

You can choose not to provide us with your personal data. However, please note that if you do not provide this information, you may not be able to take full advantage of some of the features of our services or our website. It is important to note that the provision of personal data is voluntary. You have the right to withdraw your consent at any time, in which case you should contact us using the contact details provided in this policy.

WHY DO WE COLLECT YOUR PERSONAL DATA?

We may collect your personal data when required by law but generally we collect personal data from you (or about you) to allow us to:

- supply you with information about our products and services;
- provide you with our products and services;
- ensure your use of our services and products are safe and secure;
- send administrative information to you;
- respond to inquiries and offer support;
- improve user experience;

- enforce terms and conditions and policies;
- protect from abuse and malicious users;
- respond to legal requests and prevent harm;
- communicate more effectively with you about our services; and
- ensure your experience with us is a positive one.

Personal data collected or received by us will only be used for the stated purpose for which it was provided.

WHEN DO WE DISCLOSE YOUR PERSONAL DATA?

We may collect, hold, use and disclose your personal data for the following purposes:

- to enable you to access and use our services and products;
- to enable our chosen third party service providers to work with us in delivering our products and services to you such as your healthcare team;
- to send you service, support and administrative messages, reminders, technical notices, updates, security alerts, and information requested by you; and
- to comply with our legal obligations, including but not limited to the Act and APPs, resolve any disputes that we may have with any of our users, and enforce our agreements with third parties.

TO WHOM DO WE DISCLOSE YOUR PERSONAL DATA?

We may share your Sensitive Data relating to:

- your health to other medical service providers, such as your general practitioner or specialist medical practitioners.
- in circumstances where it is required for the delivery of health services to you such as other health service providers;
- billing obligations and liaising with government departments regarding payments;
- where it is necessary to prevent or lessen a serious threat to a patient's life, health or safety; or
- any other reason as permitted by law.

We may disclose your Sensitive Data to third party AI service providers whom we engage to review your military medical records. We will only supply this information with your express written consent.

We may disclose personal data for the purposes described in this privacy policy to:

- our employees, agents and contractors and related bodies corporate;
- third party suppliers and service providers (including providers for the operation of our website and/or our business or in connection with providing our services to you) including banks and payment processors and service provider;
- businesses whom you interact with via our services;
- professional advisers and agents;

- our existing or potential third party service providers, agents, business partners or partners;
- anyone to whom our assets or businesses (or any part of them) are transferred;
- specific third parties authorised by you to receive information held by us; and/or
- other persons, including government agencies, regulatory bodies and law enforcement agencies, or as required, authorised or permitted by law.

If personal data is disclosed to a third party, we commit to taking all necessary measures to ensure your personal data is handled in compliance with the privacy laws applicable in the recipient country. We may disclose your personal data to a trusted third party who also holds other information about you. This third party may combine that information to enable it and us to develop anonymised consumer insights, with the aim of better understanding your preferences and interests, personalising your experience, and improving the products and services that you receive, provided we have obtained your explicit consent beforehand.

WHAT IF YOU DON'T WANT US TO COLLECT YOUR PERSONAL DATA?

You are not obligated to provide us with your personal data. You may choose whether you receive communications from us. Whilst it is your choice not to provide your personal data to us this may impede our ability to provide you with all the functionality of our services and website.

WHAT IF YOU DON'T WANT TO RECEIVE FURTHER COMMUNCATIONS FROM US?

Should you wish to remove yourself from our database you may do so at any time by contacting us by emailing us at contact@drvc.com.au.

HOW CAN I ACCESS, CORRECT AND/ OR UPDATE PERSONAL DATA YOU HAVE COLLECTED?

At any time, you may contact us to request your personal data be modified. We will make all efforts to correct data once we have proved your identity. Once any corrections are made to your personal data, we will notify you via email or your preferred method of communication to confirm that the changes have been implemented. We do not charge any fees for processing access or correction requests or submit corrections.

To submit corrections to your personal data, please email our Privacy Officer at contact@drvc.com.au with the subject line "Personal Data Correction Request". In your email, please include your full name, contact information, the specific data you wish to correct, and the accurate information. We will verify your identity and process your correction request as quickly as possible, making all efforts to correct the data once we have confirmed your identity and the accuracy of the new information.

We will deal with all requests for access to personal data as quickly as possible, but no later than the prescribed time required by law (unless any complexities arise). Requests for a large amount of information, or information which is not currently in use, may require further time before a response can be given.

We will provide you your personal data in a structured, commonly used, machine-readable format.

In certain circumstances, we may refuse to provide you with access to the personal data we hold about you. Such circumstances include, but are not limited to situations where providing access would be:

- unlawful;
- unreasonably impact other people's privacy;
- compromise an investigation of unlawful activity;
- disclose our intentions that could affect negotiations with you;

- hinder enforcement-related activities conducted by or on behalf of an enforcement body; or
- reveal evaluative information connected with a commercially sensitive decision-making process within our business.

We will also refuse access where the personal data relates to existing or anticipated legal proceedings, and the information would not be accessible by the process of discovery in those proceedings. Further, we reserve the right to refuse access if we find that your request is frivolous or vexatious, or if we have a reasonable belief that there is an ongoing or potential unlawful activity or serious misconduct that could be impacted detrimentally by granting access.

If we refuse to give you access, we will provide you with reasons for our refusal, unless doing so would be unreasonable in the circumstances. We will also take reasonable steps to give you access in a way that meets your needs without giving rise to the reasons of our refusal. Further, we will provide details of how you may make a complaint about our decision.

Please note that the access and correction requirements under this Privacy Policy operates alongside and do not replace other informal or legal procedures by which an individual can be provided access to, or correction of, their personal data. We maintain a record of all access and correction requests received, along with their outcomes, for internal audit and compliance purposes.

We may ask you to verify your identity before acting on any of your requests. We will not charge a fee for the exercise of your rights under the Act. However, we may charge a reasonable fee if your request involves a significant amount of work. Unless permitted by the Act, we will not refuse to comply with your request.

HOW DO WE STORE AND PROTECT YOUR PERSONAL DATA?

Transmitting personal data via the internet does have inherent risks associated with it. We will take all reasonable steps, including but not limited to the use of encryption, secure servers, and two-factor authentication, to ensure the security of this data.

We have taken the necessary measures to ensure the personal data we hold is not compromised. In accordance with and as permitted by applicable law and regulations we will retain your information as long necessary to provide our services to you or as otherwise required to operate our service.

We have established agreements with third parties that require them to maintain adequate security measures and we conduct regular audits to verify compliance. However, we cannot be held liable for events outside our control.

Our website is protected by SSL security certificates during data transfer along with 2FA, and is built considering all modern security standards, including the use of encryption and secure servers where possible. We will take reasonable steps to maintain the integrity and security of any personal data we have stored, including taking reasonable steps to prevent interference and loss, misuse, unauthorised access, modification or disclosure of such personal data.

Note that no information transmitted over the Internet can be guaranteed to be completely secure. While we will endeavour to protect your personal data as best as possible, we cannot guarantee the security of any information that you transmit to us or receive from us. The transmission and exchange of information is carried out at your own risk.

It is important that you protect your privacy by ensuring that no one obtains your personal data, and you must contact us directly if your details change. Should your information be erroneously provided to us or no longer remain valid within the constraints of this Privacy Policy we will securely destroy or de-identify it as soon as practicable, as long as it is lawful to do so.

We have obligations to notify you if you are affected by a data breach. We will take all reasonable precautions to take remedial action to prevent such an event. However, as we cannot guarantee that remedial action will be sufficient to prevent all instances of a breach, we will take steps to notify you of

an eligible data breach as soon as practicable, and provide recommendations as to what steps you should take to mitigate any serious issues.

HOW LONG DO WE KEEP YOUR PERSONAL DATA

We are committed to regularly reviewing and updating our data retention periods to ensure compliance with legal requirements and best practices in data protection. Personal data shall be processed and stored for as long as required by the purpose they have been collected for. We ensure that personal data is minimised to what is necessary during the retention period and securely deleted or anonymised when no longer needed.

Therefore:

- Personal data collected for purposes related to the performance of a contract between us and you shall be retained until such contract has been fully performed.

- Personal data collected for the purposes of our legitimate interests shall be retained as long as needed to fulfil such purposes. You may find specific information regarding the legitimate interests pursued by us within the relevant sections of this document or by contacting us.

We will retain personal data for a longer period if we are required to do so by law or by an order from a legal authority. Exceptions to our standard retention periods may apply in cases of ongoing legal disputes, investigations, or other legitimate business needs that require extended retention. In such cases, we will retain the relevant data only for as long as necessary to fulfill these specific purposes. Once the retention period expires, personal data shall be automatically deleted through our data management system. The right of access, the right to erasure, the right to rectification and the right to data portability cannot be enforced after expiration of the retention period.

YOUR RIGHTS ABOUT YOUR PERSONAL DATA

You may exercise certain rights regarding their personal data which we process. In particular, you have the right to do the following:

- You have the right to withdraw consent where you have previously given your consent to the processing of your personal data.

- You have the right to object to the processing of your personal data if the processing is carried out on a legal basis other than consent.

- You have the right to learn if your personal data is being processed by us, obtain disclosure regarding certain aspects of the processing and obtain a copy of the personal data undergoing processing.

- You have the right to verify the accuracy of your personal data and ask for it to be updated or corrected.

- You have the right, under certain circumstances, to restrict the processing of your personal data. In this case, we will not process your personal data for any purpose other than storing it.

- You have the right, under certain circumstances, to obtain the erasure of your personal data from us.

- You have the right to lodge a complaint with the Office of the Australian Information Commissioner (**OAIC**).

LOG DATA

Whenever you use our website, or in a case of an error within the website, we collect data and information (through third party products) called Log Data. This Log Data may include information such

as your device, Internet Protocol address, device name, operating system version, the configuration of the device when utilising our website, the time and date of your use of our website and other statistics.

TRANSFER OUT

We may transfer personal data we receive about you to:

- our hosting service providers and data centres and such data centres may be located overseas; and
- our third party service providers who assist us in analysing and reporting back to us on the personal data you provide to us.

Such transfers are subject to compliance with the Australian Privacy Principles, specifically APP 8 – Cross-border Disclosure of Personal Information. You acknowledge that such transfers may occur, and that any data that we transfer may be subject to laws, regulations, and standards that are different from those in your country. We will comply with all applicable data localisation requirements in the jurisdictions where we operate. Where required by law, certain data may be stored locally in your country of residence. We will take all reasonable steps to ensure that your data is treated securely and in accordance with this Privacy Policy.

We will notify you of any changes in the law that may affect our international data transfers. If such changes occur, we may need to implement additional safeguards or alter our data transfer practices to remain compliant with applicable laws and regulations. We will keep you informed of any significant changes that may impact the processing of your personal data.

You have the right to object to the international transfer of your personal data. If you wish to exercise this right, please contact us at contact@drvc.com.au. We will consider your objection and, where possible, accommodate your request. However, please note that in some cases, we may need to transfer your data outside of Australia to provide our services effectively.

You acknowledge that personal data that you submit for publication through our website or products or services may be available, via the internet, around the world. We will take reasonable steps to prevent the use (or misuse) of such personal data by others.

USE OF AI SERVICE PROVIDERS

We may engage third-party AI service providers (for example, Coral AI at https://www.getcoralai.com/) to process, analyse, and summarise personal and sensitive health information on our behalf. This may involve the cross-border disclosure of information to countries such as the United States where these providers are based.

All data uploaded to our AI service providers is encrypted at rest with AES-256 encryption and encrypted in transit via TLS. We only engage providers who commit that your data will never be used to train AI models or algorithms.

Our AI service providers retain and delete data according to their published policies:

- Coral AI: Data stored in the US; retained and deleted per https://www.getcoralai.com/privacy-policy.
- OpenAI: Inputs/outputs retained up to 30 days for service provision, then deleted unless legal obligations require retention – see https://openai.com/enterprise-privacy/.
- Anthropic: See https://privacy.anthropic.com/en/articles/10023548-how-long-do-you-store-personal-data.
- Azure OpenAI: See https://learn.microsoft.com/en-us/legal/cognitive-services/openai/data-privacy?tabs=azure-portal.

- Google Vertex AI: Prompts and tuning data never used to train foundation models – see https://cloud.google.com/vertex-ai/generative-ai/docs/multimodal/multimodal-faqs.

- Amazon Bedrock: Does not log or use prompts/completions to train AWS models – see https://docs.aws.amazon.com/bedrock/latest/userguide/data-protection.html.

We will comply with APP 8 (Cross-border Disclosure) when transferring personal and sensitive health information to AI service providers overseas. We take all reasonable steps to ensure that overseas recipients handle your data in accordance with Australian Privacy Principles and equivalent data security standards.

CHANGES TO THIS PRIVACY POLICY

We reserve the right to modify or amend this Privacy Policy at any time. If we make any material changes, we will notify you by email (sent to the e-mail address specified in your account) or by means of a notice on this website prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.

If you object to any changes, you may cease using our website and/or our services. You acknowledge and agree that your continued use of our website means that the collection, use and sharing of your personal data is subject to the updated Privacy Policy.

ENQUIRIES, REQUESTS & COMPLAINTS

Enquiries regarding this Privacy Policy or the personal data we may hold on you, should be addressed to the Privacy Officer at contact@drvc.com.au.

If you think your personal data, held by us, may have been compromised in any way or you have any other Privacy related complaints or issues, you should also raise the matter with the Privacy Officer.

We will ensure your claims are investigated and a formal response will be provided to you, within a reasonable time, considering the circumstances of your claims. If any corrective action is determined to be required, as a result of that investigation, we will take all reasonable steps to rectify the situation and advise you of such, again within a reasonable time considering the circumstances.

If we do not resolve your enquiry, concern or complaint to your satisfaction or you require further information in relation to any privacy matters, please contact the Office of the Australian Information Commission, whose contact details are below.

Office of the Australian Information Commission

Telephone	1300 363 992
Email	enquiries@oaic.gov.au
Office Address	Level 3, 175 Pitt Street, Sydney NSW 2000
Postal Address	GPO Box 5218, Sydney NSW 2001
Website	www.oaic.gov.au

LAST UPDATED: 10 May 2025