



With me.
With you.

OUR PRIVACY POLICY

INTRODUCTION

Here at With Me With You Pty Ltd ACN 689 699 590 (**we, us or our**) protecting your privacy and treating your personal information in accordance with Australian privacy laws is of paramount importance to us. This Privacy Policy explains what personal information we collect, why we collect personal information and how we collect, use, disclose, store and protect your personal information when you visit our website, use our specialist general practitioner services for Australian Defence Force (ADF) veterans, provide us with information yourself such as when you first become a patient of our practice, or continue to use our services for the Department of Veterans' Affairs (DVA) medical assessments.

As healthcare providers registered with AHPRA and Fellows of the Royal Australian College of General Practitioners, we are committed to maintaining the highest standards of privacy protection for sensitive health information. Our practice specialises in providing medical services to serving and ex-serving ADF personnel, including assistance with DVA claims and compensation assessments.

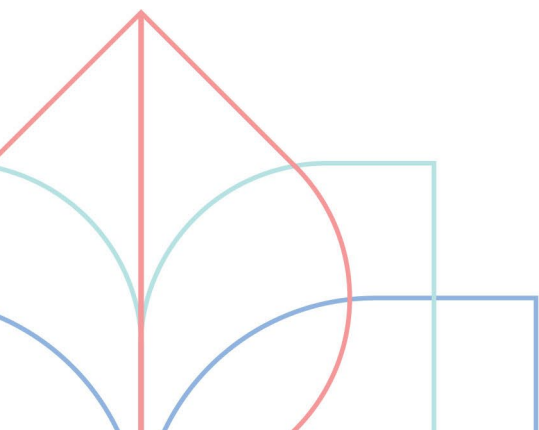
Our Privacy Policy also explains how to contact us to correct, update or delete any personal information provided to us, or make a complaint if you have concerns. We are compliant with the *Privacy Act 1988* (**Privacy Act**).

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.

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 information. If you do not agree with the changes, you may choose to stop using our services.





With me.
With you.

COLLECTION OF YOUR PERSONAL INFORMATION BY THIRD PARTIES

This Privacy Policy does not apply to any third-party service 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.

WHICH ENTITIES DOES THIS PRIVACY POLICY COVER?

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

WHAT IS PERSONAL INFORMATION?

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

WHEN AND HOW DO WE COLLECT YOUR PERSONAL INFORMATION?

We collect most personal information directly from you when you consent to use our services or receive communications from us, or information we receive from third parties (for instance from your treating General Practitioner or other health care provider). Your consent may be express (e.g. you agree to the use of your information by ticking a box when you become a patient) 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).

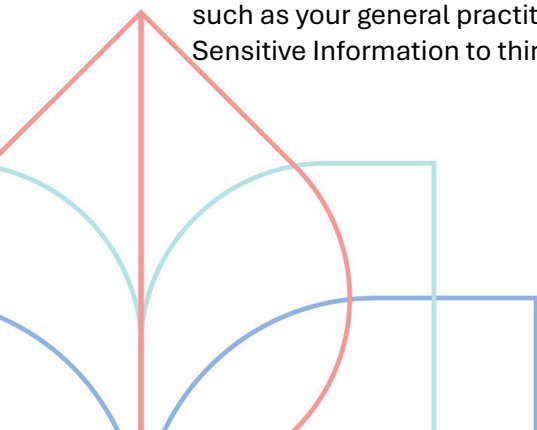
You provide us your information when you use our services or you use our website generally or you deal with us.

WHAT PERSONAL INFORMATION DO WE COLLECT?

Personal Information

We may collect and process various types of personal information, including sensitive personal information. Sensitive personal information includes information such as racial or ethnic origin, political opinions, religious beliefs, health information, or biometric information (**Sensitive Information**). When we collect sensitive personal information, 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 may provide Sensitive Information relating to your health to other medical service providers, such as your general practitioner or specialist medical practitioners and we may disclose your Sensitive Information to third party AI service providers whom we engage to record, transcribe





With me.
With you.

and analyse our clinical sessions. We will only supply this information with your consent, or in circumstances where it is required for the delivery of health services, such as referral to another health service provider, billing and liaising with government offices regarding Medicare entitlements and payments, where it is necessary to prevent or lessen a serious threat to a patient's life, health or safety, or other reason as permitted.

We collect personal information necessary for providing specialist medical services to ADF veterans and serving members, and supporting DVA medical assessments. This includes:

Demographic and Contact Information

Your full name, date of birth, gender, occupation, residential address, postal address, telephone numbers, email address, emergency contact details, and next of kin information.

Government and Insurance Identifiers

DVA file number, Medicare number, and any relevant pension concession card details.

Health and Medical Information

We collect extensive sensitive health information including your smoking history, alcohol consumption patterns, illicit drug use history, family medical history, complete past medical history including all diagnoses and surgical procedures, known allergies and adverse reactions, current medications and treatment regimens, and mental health information including diagnoses, treatment notes, risk assessments, and standardised screening tool results.

DVA-Specific Information

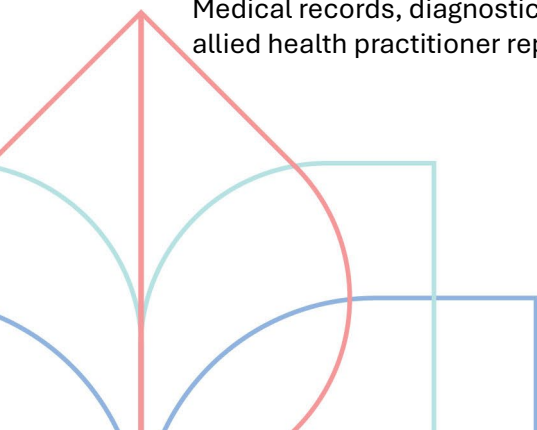
DVA accepted medical conditions, disability and impairment information specifically related to DVA diagnostic forms, diagnostic assessments, permanent impairment assessments, ability to work evaluations, and other DVA documentation required for initial liability claims processing and compensation determinations.

Clinical Assessment Data

Treatment and management plans developed specifically for your care, results from clinical assessments and examinations, pathology and imaging investigation results, specialist consultation reports, and allied health practitioner reports including mandatory end-of-cycle reports provided every twelve visits following our referrals.

Third-Party Medical Information

Medical records, diagnostic reports, treatment summaries, imaging studies, hospitals and allied health practitioner reports to support care coordination and DVA claims substantiation.





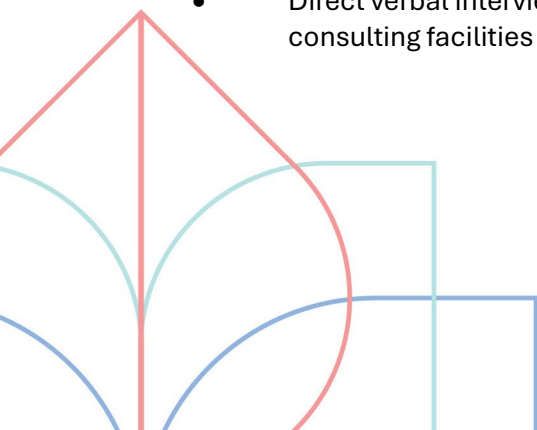
With me.
With you.

Additionally, we may collect:

- credit card and other information for billing;
- identifying information about yourself, your employees and contractors;
- if you visit our website, 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, ad information, IP address and standard web log information, and the specific purpose for which each category of information is used;
- 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 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 surveys; or
- any other personal information that is directly related to and necessary for facilitating your dealings with us, as explicitly stated at the time of collection.

Our practice employs digital collection methods designed to ensure accuracy, security, and efficiency in gathering the comprehensive information required for veteran healthcare and DVA medical assessments. We collect personal information through:

- Digital intake and consent forms administered through our secure practice management system, which capture demographic, medical, and DVA-specific information in a structured format that ensures completeness and accuracy for clinical and diagnostic assessments.
- AI-assisted clinical documentation during consultations, utilising advanced scribe technology (Lyrebird Health) that transcribes and structures clinical conversations while maintaining strict privacy protections and allowing for real-time verification of accuracy.
- Direct verbal interviews and clinical consultations conducted both in-person at our consulting facilities and via secure telehealth platforms integrated within our practice





With me.
With you.

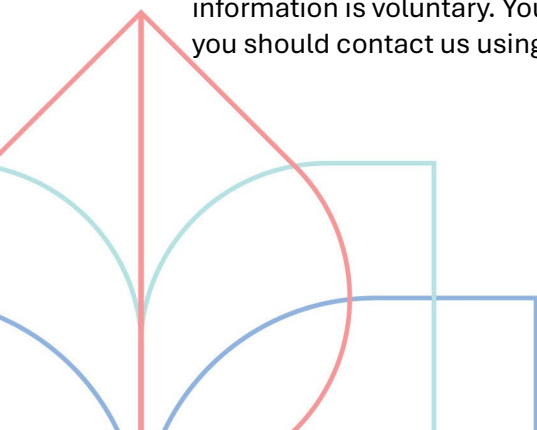
management system, ensuring consistent documentation standards regardless of consultation method.

- Clinical assessments and physical examinations performed according to DVA assessment requirements and RACGP clinical guidelines, with findings documented in standardised formats that support both clinical care and compensation assessment requirements.
- Referral documents and clinical reports received from external healthcare providers including non-GP specialists, hospitals, allied health practitioners, pathology services, and imaging providers, which are integrated into your clinical record to ensure continuity of care and assessment documentation.
- Test results and investigation reports including pathology results, diagnostic imaging studies, and specialist consultation reports that are essential for establishing diagnoses, monitoring treatment effectiveness, and supporting DVA claim substantiation.
- Information sharing arrangements with family members, support persons, or carers, implemented only with your explicit consent and documented through our secure digital consent management system.
- Patient-provided DVA correspondence and documentation, recognising that all formal communication between veterans and DVA occurs directly between those parties, with our practice receiving information only as provided by you for the purpose of clinical assessment and report preparation.

We may collect these types of personal information 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;
- communicate with us through correspondence, chats, email, or when you share information with us from other social applications, services or websites;
- interact with our site, products, services, content and advertising.

You can choose not to provide us with your personal information. 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 information 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.





With me.
With you.

Third-Party Information Sources and Veteran Advocate Relationships

Our practice receives information from various third-party sources essential for providing veteran healthcare and DVA medical assessment services. We maintain strict consent protocols for all third-party information sharing, recognising the unique relationships within the veteran community.

We receive clinical information from non-GP specialists who provide diagnostic reports, treatment records, imaging studies, and pathology results essential for supporting DVA diagnostic assessments. Allied health practitioners provide both clinical reports and mandatory end-of-cycle summaries every twelve visits following our referrals. Imaging providers supply diagnostic studies and reports that confirm diagnoses and support compensation assessments.

We frequently interact with veteran advocates, both paid and voluntary, who provide medical and service history information and assist veterans in understanding their entitlements and claim options. We recognise that paid advocates receive financial compensation based on successful claim outcomes, creating potential conflicts of interest that we manage through strict consent protocols and independent clinical assessment practices.

Veteran advocates may provide permanent impairment paperwork containing accepted diagnoses and historical medical information. We collect this information only with express written consent from the veteran and maintain clear boundaries regarding our independent clinical assessment responsibilities.

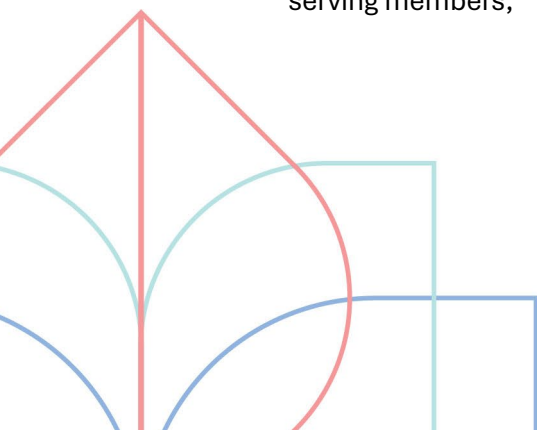
While all formal correspondence regarding claims occurs directly between veterans and DVA, DVA may occasionally contact our practice directly. In such instances, we always verify that appropriate consent has been provided and confirm authorisation with the veteran before engaging in any communication. Our only direct communication with DVA involves uploading invoices through their secure online portal system.

With appropriate authorisation, we may receive information from or provide information to legal representatives assisting veterans with compensation claims, ensuring that all communications are properly documented and consent is clearly established.

WHY DO WE COLLECT YOUR PERSONAL INFORMATION?

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

- provide you with our specialist general practitioner services for ADF veterans and serving members;





With me.
With you.

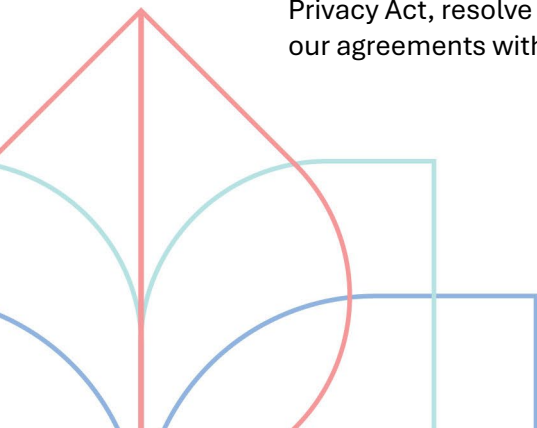
- assist with DVA diagnostic forms, diagnostic assessments and permanent impairment assessments;
- facilitate access to DVA funded treatments and services;
- provide medical referrals to non-GP specialists and allied health providers;
- ensure your use of our services are safe and secure;
- send administrative information;
- marketing and advertising to you, with your explicit consent and in compliance with the Australian Privacy Principles (**APPs**) under the Privacy Act;
- respond to inquiries and offer support;
- respond to legal requests and prevent harm;
- communicate more effectively with you about our services and your care; and
- ensure your experience with us is a positive one.

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

WHEN DO WE DISCLOSE YOUR PERSONAL INFORMATION?

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

- to enable you to access and use our services;
- to operate, protect, improve and optimise our services, business and our users' experience, such as to perform analytics, conduct research and for advertising and marketing;
- to send you service, support and administrative messages, reminders, updates and information requested by you;
- to send you marketing and promotional messages and other information that may be of interest to you; and
- to comply with our legal obligations, including but not limited to the APPs under the Privacy Act, resolve any disputes that we may have with any of our users, and enforce our agreements with third parties.





With me.
With you.

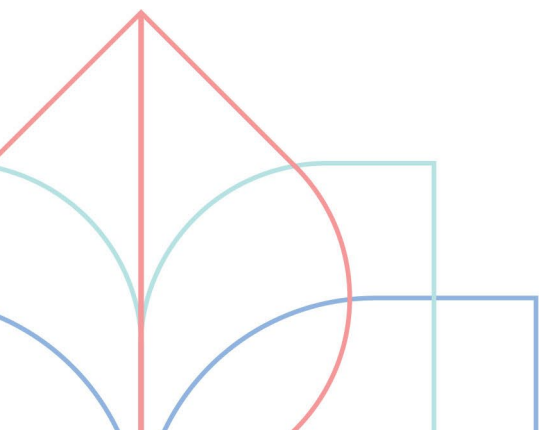
TO WHOM DO WE DISCLOSE YOUR PERSONAL INFORMATION?

We may disclose personal information 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;
- businesses whom you interact with via our services;
- your treating General Practitioner or other healthcare providers;
- DVA delegates and representatives for claims and assessment purposes (with your consent);
- veteran advocates, both paid and voluntary (with your written consent);
- specialist medical practitioners and allied health providers;
- pathology services, imaging providers, and other diagnostic services;
- payment systems operators (e.g. merchants receiving card payments);
- 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 information is disclosed to a third party, we commit to taking all necessary measures to ensure your personal information is handled in compliance with the privacy laws applicable in the recipient country.

We may disclose your personal information 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.





With me.
With you.

Consent Management for Veteran Services

Given the unique nature of veteran healthcare and the frequent involvement of advocates in the claims process, we have established consent management protocols that address the specific needs of the veteran community while ensuring full compliance with privacy requirements.

Standard Consent Procedures

All patients complete digital intake and consent forms that specifically address consent for communication with DVA delegates, veteran advocates (both paid and voluntary), and family members or support persons. This streamlined approach recognises that the majority of our patients work with advocates and require frequent communication with DVA throughout the claims process.

Advocate Communication Consent

Our intake process includes specific consent provisions for communication with veteran advocates, acknowledging the important role these individuals play in supporting veterans through the claims process. We clearly explain the distinction between paid advocates (who receive financial compensation based on claim outcomes) and voluntary advocates, ensuring veterans understand any potential conflicts of interest.

DVA Communication Authorisation

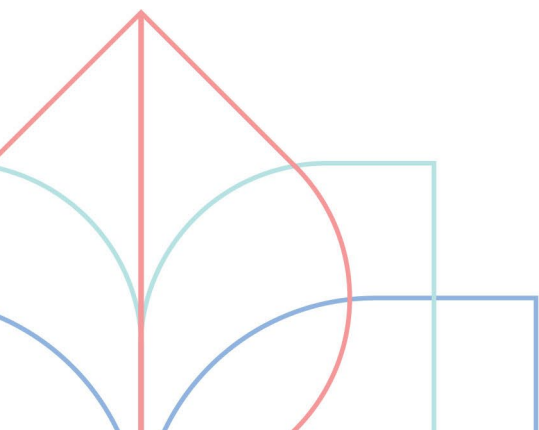
We obtain specific consent for communication with DVA delegates and for uploading assessment reports and documentation directly to DVA systems. Veterans are informed that while we may receive direct contact from DVA, we always verify consent before engaging in any substantive communication.

Dynamic Consent Management

For situations requiring additional consent beyond our standard intake procedures, we utilise secure digital consent systems that can be delivered via SMS or email, creating documented consent records within the patient's clinical file. We maintain preference for digital consent documentation over verbal consent, though both methods are available when clinically appropriate.

Capacity and Substitute Decision-Making

For veterans who may lack capacity to provide informed consent, we engage with legally appointed carers, Enduring Powers of Attorney, or other authorised decision-makers in accordance with relevant state and territory legislation and AHPRA guidelines.





With me.
With you.

AGGREGATED INFORMATION & DIRECT MARKETING

We do not sell your personal information. However, we may aggregate the information you and others provide to us and share this aggregated information with third parties.

We may use and share this aggregated information with third parties for research purposes or to enhance our services and provide our partners with a better understanding of the users of our services. We will not sell or licence this aggregated information.

You can object to us using your information for these purposes.

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

You are not obligated to provide us with your personal information. You may choose whether you receive communications from us. Whilst it is your choice not to provide your personal information 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 COMMUNICATIONS 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 operations@withyou.com.au.

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

Accessing and Correcting Your Personal Information

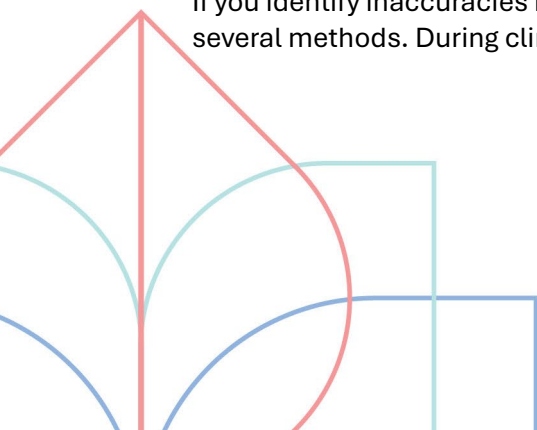
You have rights regarding your personal information held by our practice, and we have established clear procedures to facilitate the exercise of these rights in accordance with the Privacy Act and the enhanced individual rights framework introduced in 2024.

Access to Personal Information

You may request access to your personal information at any time by contacting our Privacy Officer at operations@withyou.com.au. We will provide access to your information within the timeframes required by law, typically within 30 days of receiving your request. Access may be provided through secure digital delivery, in-person review at our practice, or through other methods that ensure security and confidentiality.

Correction of Personal Information

If you identify inaccuracies in your personal information, you may request corrections through several methods. During clinical consultations, corrections can be made immediately and





With me.
With you.

documented in your clinical record. Outside of consultations, you may submit correction requests via secure digital forms delivered through SMS or email from our practice management system, or by contacting our Privacy Officer directly.

Information Deletion Requests

You may request deletion of your personal information in circumstances where retention is no longer required for clinical care, legal obligations, or professional requirements. We will assess each deletion request against our legal and professional obligations, including healthcare record retention requirements and potential DVA assessment review needs. Where deletion is not possible due to legal or professional obligations, we will explain the reasons and explore alternative approaches such as restricting access or use.

Restricting Use or Disclosure

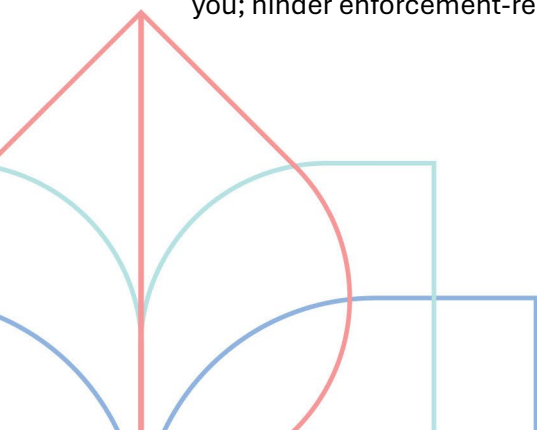
You may request restrictions on how we use or disclose your personal information. We will accommodate such requests where possible while maintaining our ability to provide safe and effective clinical care. Restrictions on information sharing with DVA or advocates may impact our ability to assist with claims processing, and we will discuss these implications with you before implementing any restrictions.

At any time, you may contact us to request your personal information be modified. We will make all efforts to correct information once we have proved your identity. Once any corrections are made to your personal information, 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 information, please email our Privacy Officer with the subject line “Personal Information Correction Request”. In your email, please include your full name, contact information, the specific information 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 information once we have confirmed your identity and the accuracy of the new information.

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

In certain circumstances, we may refuse to provide you with access to the personal information 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;





With me.
With you.

or reveal evaluative information connected with a commercially sensitive decision-making process within our business.

We will also refuse access where the personal information 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 information. We maintain a record of all access and correction requests received, along with their outcomes, for internal audit and compliance purposes.

HOW DO WE STORE AND PROTECT YOUR PERSONAL INFORMATION?

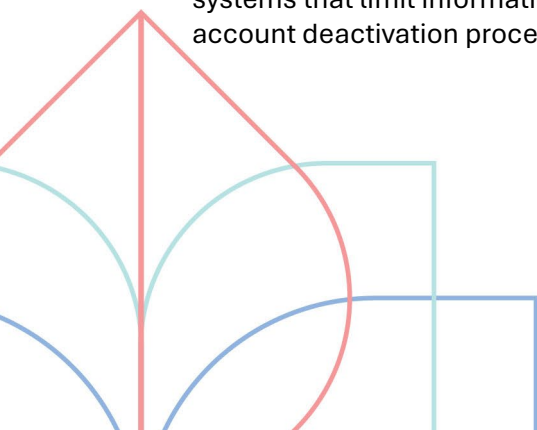
Technical Security Measures

In compliance with the enhanced requirements under Australian Privacy Principle 11 as amended by the *Privacy and Other Legislation Amendment Act 2024*, we have implemented technical security measures including multi-factor authentication for all system access, encryption of sensitive information both in transit and at rest, secure server infrastructure provided by certified cybersecurity specialists, and regular security monitoring and threat assessment protocols.

Our practice management system employs enterprise-grade security features including role-based access controls, audit logging of all information access and modifications, automated backup systems with encryption, and secure remote desktop access for cloud-based operations. All clinical information is stored within Australian data centres with appropriate sovereignty protections.

Organisational Security Measures

We have established organisational security protocols including structured access privilege systems that limit information access based on clinical need and role requirements, immediate account deactivation procedures when staff members leave the organisation, regular staff





With me.
With you.

training on privacy and security obligations, and documented incident response procedures for potential security breaches.

Our cybersecurity framework is developed and maintained in partnership with Australian Cyber Defence, an endorsed cybersecurity expert, ensuring compliance with medical practice security standards and RACGP accreditation requirements. We conduct regular security assessments and maintain current cyber insurance coverage through Avant Insurance.

We employ:

- conditional access protocols allowing access to personal information from designated pre-approved locations
- restricted access to files based on approved listings to prevent accidental deletion
- device control and monitoring to ensure data is unable to be exported from our systems.

Information Handling Protocols

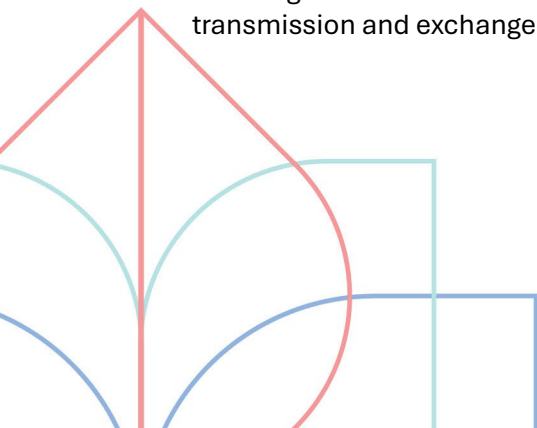
All patient emails are immediately imported into our secure practice management system and deleted from external email accounts to minimise exposure risks. We maintain strict protocols for handling DVA documentation and permanent impairment assessments, with direct upload to DVA systems and no retention of copies outside our secure clinical record system.

Our AI-assisted documentation systems (Heidi platforms) operate under strict privacy agreements with information processing occurring within Australian jurisdictions and immediate deletion of temporary processing files following clinical documentation completion.

We have taken the necessary measures to ensure the personal information 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 serve you, to maintain your account or as otherwise required to operate our service. We have established agreements with these 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.

We will take reasonable steps to maintain the integrity and security of any personal information we have stored, including taking reasonable steps to prevent interference and loss, misuse, unauthorised access, modification or disclosure of such personal information.

Note that no information transmitted over the Internet can be guaranteed to be completely secure. While we will endeavour to protect your personal information 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.





With me.
With you.

It is important that you protect your privacy by ensuring that no one obtains your personal information, 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 INFORMATION

Information Retention Periods

As a healthcare provider operating in the Australian Capital Territory and providing services to veterans across Australia, we maintain personal information in accordance with healthcare record retention requirements and professional obligations.

Standard Retention Period

We retain all clinical records and personal information for a minimum of seven years after the date of the last clinical entry. For patients who were minors at the time of treatment, we retain records until the patient attains or would have attained the age of 25 years, or for a minimum of seven years after the date of the last entry, whichever period is longer.

DVA Assessment Records

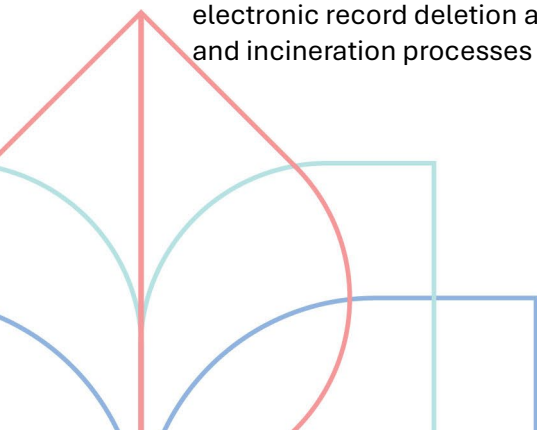
Permanent impairment assessments, diagnostic assessments and DVA-related documentation are retained for the same periods as clinical records, recognising that these assessments may be subject to review or appeal processes that could extend beyond standard timeframes.

Consent and Communication Records

Records of consent for information sharing, communication with advocates, and DVA correspondence are retained for the same period as the associated clinical records to ensure continuity of care and legal protection.

Secure Disposal Procedures

When authorised for disposal, we destroy material containing patient health information through consultation with our IT service provider to determine appropriate methods for electronic record deletion and device disposal. Paper records are destroyed through shredding and incineration processes that ensure patient identification is impossible. We engage certified





With me.
With you.

secure destruction services that provide written certification of secure destruction for all disposed records.

Legal Hold Exceptions

Retention periods may be extended when records are subject to legal proceedings, regulatory investigations, or other circumstances where disposal would be inappropriate or unlawful.

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

Therefore:

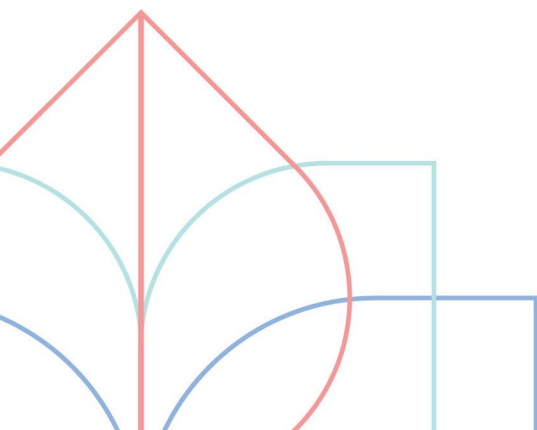
- Personal Information collected for purposes related to the performance of a contract between us and you shall be retained until such contract has been fully performed.
- Personal information collected for the purposes of our legitimate interests shall be retained as long as needed to fulfil such purposes. 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 information 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 information only for as long as necessary to fulfil these specific purposes.

Once the retention period expires, personal information shall be automatically deleted through our information management system. The right of access, the right to erasure, the right to rectification and the right to information portability cannot be enforced after expiration of the retention period.

Automated Decision Making and AI-Assisted Services

In compliance with the *Privacy and Other Legislation Amendment Act 2024* requirements for automated decision making disclosure, we inform you of the following automated systems that may impact your care:





With me.
With you.

AI-Assisted Clinical Documentation

We utilise AI-powered clinical scribe technology (Lyrebird Health) to assist with clinical documentation during consultations. These systems transcribe and structure clinical conversations but do not make clinical decisions or assessments. All clinical decisions remain under the direct control of our qualified medical practitioners.

Practice Management Automation

Our practice management system includes automated features for appointment scheduling, billing processes, and communication delivery. These systems operate under predefined parameters and do not make decisions that would negatively impact your care or access to services.

No Automated Clinical Decision Making

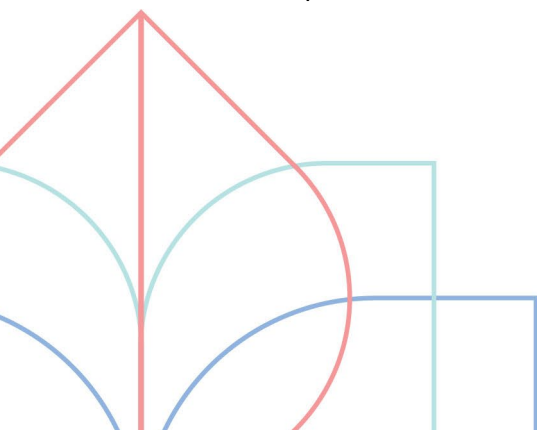
We do not utilise automated systems for clinical decision making, diagnosis, treatment recommendations, or DVA medical assessment determinations. All clinical assessments, permanent impairment evaluations, and treatment decisions are made by qualified medical practitioners using professional clinical judgement.

You have the right to request human review of any automated processes and to understand how these systems operate in relation to your care. We will provide additional information about our automated systems upon request.

YOUR RIGHTS ABOUT YOUR PERSONAL INFORMATION

You may exercise certain rights regarding their personal information 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 information.
- You have the right to object to the processing of your personal information if the processing is carried out on a legal basis other than consent.
- You have the right to learn if your personal information is being processed by us, obtain disclosure regarding certain aspects of the processing and obtain a copy of the personal information undergoing processing.
- You have the right to verify the accuracy of your personal information and ask for it to be updated or corrected.





With me.
With you.

- You have the right, under certain circumstances, to restrict the processing of your personal information. In this case, we will not process your personal information for any purpose other than storing it.
- You have the right, under certain circumstances, to obtain the erasure of your personal information from us.
- You have the right to lodge a complaint with the Office of the Australian Information Commissioner (OAIC).

Complaint Procedures

If you have concerns about how we handle your personal information, you may lodge a complaint with our Privacy Officer at operations@withyou.com.au. We will investigate all complaints promptly and provide a formal response within a reasonable timeframe considering the circumstances. If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner (OAIC) at enquiries@oaic.gov.au or 1300 363 992.

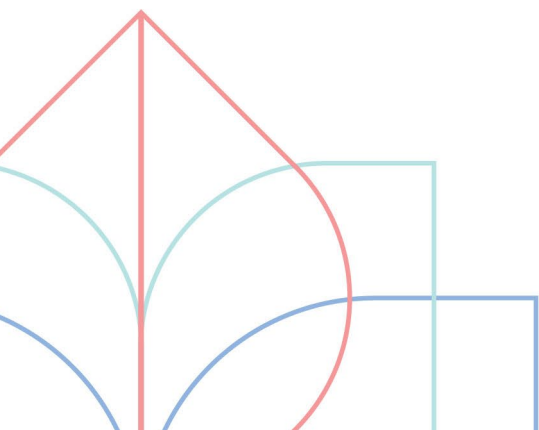
Data Breach Response and Notification

We maintain a data breach response plan that complies with the enhanced notification requirements under the Privacy Act and the strengthened enforcement framework introduced in 2024.

Upon discovery of a potential data breach, our response team immediately gathers and documents all available details about the nature, scope, timing, duration, and format of the breach. This includes identifying the person or organisation reporting the breach, documenting any immediate response actions taken, and conducting forensic analysis of information access or information transfer where appropriate.

We immediately contact our medical defence organisation (Avant) for advice and notification, ensuring that professional indemnity and cyber insurance coverage is activated where appropriate. We also engage our cybersecurity partners (Australian Cyber Defence) to assist with technical assessment and remediation.

We assess whether the breach is likely to result in serious harm to affected individuals within the required timeframes, typically within 30 days of discovery. Where possible, we undertake immediate remedial action to prevent or minimise the likelihood of serious harm. If remedial action cannot prevent serious harm, we notify affected individuals and the Office of the Australian Information Commissioner (OAIC) as soon as practicable.





With me.
With you.

Given the sensitive nature of veteran health information and the potential impact on DVA claims and compensation, we provide specialised support to affected veterans, including assistance with understanding potential impacts on their claims and coordination with DVA where appropriate and consented.

Following any breach incident, we conduct reviews to identify systemic problems, address deficiencies in our information management practices, assess the effectiveness of our response procedures, and implement improvements to prevent future incidents.

LOG DATA

Whenever you use our website, or in a case of an error within the website, we collect information 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.

Website and Digital Platform Privacy

Our website includes contact forms collecting names, email addresses, and messages from prospective patients. This information will be used solely for responding to enquiries and will be subject to the same security and privacy protections as all other personal information.

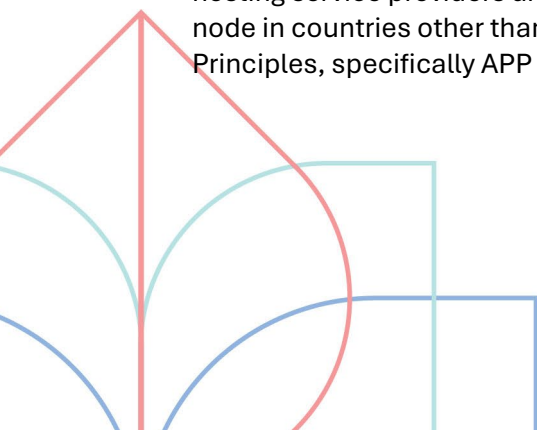
We integrate online booking functionality with our practice management system (Zanda), allowing patients to schedule appointments through secure web interfaces. All booking information will be directly integrated into our clinical record system and protected under our privacy framework.

Our website may utilise cookies and analytics tools to improve user experience and understand website usage patterns. We will implement cookie consent management systems and provide clear information about the types of cookies used, their purposes, and options for managing cookie preferences.

We utilise secure digital communication for appointment confirmations, cancellations, and reminders via SMS and email. These communications are generated through our practice management system and are subject to our standard privacy protections and security measures.

TRANSFER OUT

We may transfer information we receive about you, including all personal information, to our hosting service providers and data centres located overseas, such as an Amazon Web Services node in countries other than Australia, subject to compliance with the Australian Privacy Principles, specifically APP 8 – Cross-border Disclosure of Personal Information. You





With me.
With you.

acknowledge that such transfers may occur, and that any information 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 information localisation requirements in the jurisdictions where we operate. Where required by law, certain information may be stored locally in your country of residence. We will take all reasonable steps to ensure that your information is treated securely and in accordance with this Privacy Policy. Transfers out of your country will be protected by appropriate safeguards, these include one or more of the following: the use of standard information protection clauses adopted or approved by the European Commission which you can obtain from the European Commission Website and European Union Data Protection Agreement.

We will notify you of any changes in the law that may affect our international information transfers. If such changes occur, we may need to implement additional safeguards or alter our information 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 information.

You have the right to object to the international transfer of your personal information. If you wish to exercise this right, please contact us using the information provided in the “Contact Us” section of this Privacy Policy. We will consider your objection and, where possible, accommodate your request. However, please note that in some cases, we may need to transfer your information to provide our services effectively.

You acknowledge that personal information 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 information by others.

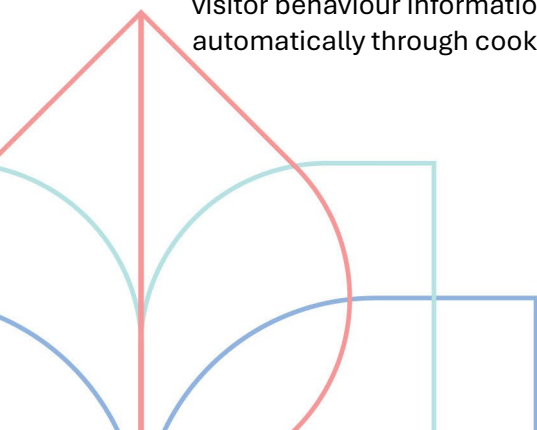
CHANGES TO THIS PRIVACY POLICY

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 information is subject to the updated Privacy Policy.

COOKIES

Cookies are text files placed on your computer to collect standard Internet log information and visitor behaviour information. When you visit our website, we may collect information from you automatically through cookies or similar technology. While we do not use browsing information





With me.
With you.

to identify you personally, we may record certain information about your use of our website, such as which pages you visit, the time and date of your visit and the internet protocol address assigned to your computer.

Insofar as those cookies are not strictly necessary for the provision of our website and services, we will ask you to consent to our use of cookies when you first visit our website. We may also use 'cookies' or other similar tracking technologies on our website that help us track your website usage and remember your preferences. Cookies are small files that store information on your computer, TV, mobile phone or other device. They enable the entity that put the cookie on your device to recognise you across different websites, services, devices and/or browsing sessions. You can disable cookies through your internet browser but our websites may not work as intended for you if you do so.

Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.

COOKIES THAT WE MAY USE

We use cookies for the following purposes:

- authentication and status - we use cookies to identify you when you visit our website and as you navigate our website, and to determine if you are logged into the website;
- personalisation - we use cookies to store information about your preferences and to personalise the website for you;
- security - we use cookies as an element of the security measures used to protect user accounts, including preventing fraudulent use of login credentials, and to protect our website and services generally;
- analysis - we use cookies to help us to analyse the use and performance of our website and services; and
- cookie consent - we use cookies to store your preferences in relation to the use of cookies more generally.

COOKIES USED BY OUR SERVICE PROVIDERS

Our service providers use cookies and those cookies may be stored on your computer when you visit our website.





With me.
With you.

MANAGING COOKIES

Most browsers allow you to refuse to accept cookies and to delete cookies. The methods for doing so vary from browser to browser, and from version to version. You can however obtain up-to-date information about blocking and deleting cookies via these links:

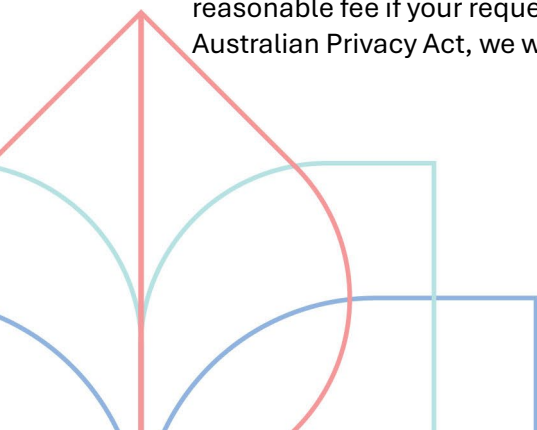
- <https://support.google.com/chrome/answer/95647> (Chrome);
- <https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences> (Firefox);
- <https://help.opera.com/en/latest/security-and-privacy/> (Opera);
- <https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-cookies> (Internet Explorer);
- <https://support.apple.com/en-gb/guide/safari/manage-cookies-and-website-data-sfri11471/mac> (Safari); and
- <https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy> (Edge).

Blocking all cookies will have a negative impact upon the usability of many websites. If you block cookies, you will not be able to use all the features on our website.

You have the following rights under the Australian Privacy Act:

- to be informed how your personal information is being used;
- access your personal information (we will provide you with a free copy of it);
- to correct your personal information if it is inaccurate or incomplete;
- to delete your personal information;
- to restrict processing of your personal information;
- to retain and reuse your personal information for your own purposes; and
- to object to your personal information being used.

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 Australian Privacy Act. However, we may charge a reasonable fee if your request involves a significant amount of work. Unless permitted by the Australian Privacy Act, we will not refuse to comply with your request.





With me.
With you.

ENQUIRIES, REQUESTS & COMPLAINTS

Privacy Officer and Contact Information

Privacy Officer: Chloe Wind

Email: admin@withmewithyou.com.au

Phone: (02) 5154 3000

Address: Unit 7 13 Napier Close Deakin ACT 2600

Practice Website: <https://withmewithyou.com.au>

Practice Name: With Me With You Pty Ltd

ABN: 14 689 699 590 | ACN: 689 699 590

For all privacy-related enquiries, access requests, correction requests, complaints, or concerns about how we handle your personal information, please contact our Privacy Officer using the details above. We are committed to responding to all privacy-related communications promptly and professionally.

If you think your personal information, 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.

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 Privacy Commissioner Australia, whose contact details are below.

Office of the Australian Information Commissioner

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

DATE OF CURRENT VERSION: 01 July 2026

