Privacy Policy

1. About this Privacy Policy

Applied Recovery Co (we or us) is bound by the Privacy Act 1988 (the Privacy Act) and the requirements of the Australian Privacy Principles (APPs) in Schedule 1 of the Privacy Act, including amendments through 2024. Under APP 1, we are required to have a Privacy Policy about how we manage personal information, as defined in the Privacy Act.

This Privacy Policy provides detailed information about our personal information handling practices, including:

- the kinds of personal information that we collect and hold
- how we collect and hold your personal information
- the purpose for which we collect, hold, use and disclose your personal information
- personal information that may be disclosed to overseas recipients
- how you can contact us if you want to access or correct personal information that we hold about you
- how you can complain about a breach of the Privacy Act and how we will respond to your complaint.

This Privacy Policy is only intended to cover how we handle personal information. It is not intended to cover how we handle other types of information.

If you would like to access this Privacy Policy in an alternate format, please contact us using the contact details set out at the end of this document.

2. What we do

Our mission is to improve the health and wellness of individuals struggling with alcohol dependence, and make withdrawal (detox) and recovery services accessible to every Australian who needs them, irrespective of postcode or socio-economic status.

We have established the Clean Slate Clinic, which delivers at-home alcohol withdrawal and recovery services, supported by a client app, and telehealth technology. Further information about the Clean Slate Clinic can be found on our website.

3. Our obligations under the Privacy Act

This Privacy Policy explains how we comply with the Privacy Act.

The Privacy Act sets out 13 APPs (Australian Privacy Principles) which regulate how we collect, use, disclose and store your personal information, and how you may access and correct personal information we hold about you.

As a healthcare provider, we are bound by the APPs in the Privacy Act, the Privacy Guidelines 2024, health records legislation, and additional requirements for healthcare providers.

4. What is personal information

We may collect both personal information and sensitive information about you.

Personal information

The Privacy Act defines 'personal information' as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable whether the information or opinion is:

- true or not; and
- recorded in a material form or not.'

For example, the personal information that we collect may include:

- your name, address and contact details (for example, phone, email and fax) to communicate with you regarding the program or other potential services
- information about your personal circumstances (for example, marital status, age, gender and relevant information about your partner and children)
- information about your financial affairs (for example, payment details and bank account details)
- information about your identity (for example, date of birth)
- information about your employment (for example, occupation)
- information about your background (for example, the languages you speak and your English proficiency) in providing you with support in accessing services

- information related to any conflict of interest declarations you make (for example, including those of your immediate family members such as spouses/partners or dependants)
- government identifiers (for example, Medicare number and health care identifier) in an application for access to a benefit or program
- information about your entitlements under the legislation we administer
- digital identifiers and online activity data
- location data and device information
- telehealth session recordings and data
- electronic health records and clinical documentation
- app usage patterns and preferences

Depending on the circumstances, information that does not include your name and date of birth may still be considered personal information, if it includes other information about you.

Sensitive information

Sensitive information is a subset of personal information. The Privacy Act defines 'sensitive information' as information or an opinion about a person's:

- racial or ethnic origin
- membership of a professional association or trade association
- sexual orientation or practices
- health or genetic information
- COVID-19 vaccination status
- gender identity
- immigration status

5. Collection of your personal information

Under the APPs, we will only collect personal information about you where it is reasonably necessary for, or directly related to, a function or activity performed by us. We will only collect sensitive personal information such as health information when you have consented, it is required or authorised by or under law, or where we are otherwise permitted under the Privacy Act.

We take reasonable steps to ensure that personal information we collect about you is accurate, up-to-date, complete, relevant and not misleading.

We collect your personal information only by lawful and fair means. In most cases, we will collect your personal information directly from you. However, there may be circumstances in which we will collect personal information about you from your representative (e.g. your nominated support person).

Methods of collection and notification

We collect personal information about you through a range of different channels including:

- paper-based and electronic forms (including online forms)
- video or telephone communications
- email and facsimile communications
- our website
- social media websites and accounts
- smartphone applications
- telehealth platforms and systems
- wearable devices and health monitoring tools
- electronic health record systems

When we collect your personal information, where it is reasonable to do so, we will issue you with this privacy policy explaining how we will handle your personal information.

For example, when you commence treatment with us, we will issue you with a privacy notice explaining:

- the purpose of us collecting your personal information
- the intended use of your personal information
- to whom your personal information may be disclosed
- your rights regarding your personal information
- how your information will be secured
- retention periods for your information
- whether your information may be sent overseas

Collecting your personal information from third parties

In accordance with the Privacy Act, we will only collect your personal information from a third party where you consent, where required or authorised by or under law or court/tribunal order, or where it is unreasonable or impracticable to collect the information only from you. For example, we may collect personal information about you from a family member with your consent.

Collection of unsolicited personal information

We may, on occasion, receive personal information about you from individuals or other entities, without it being requested by us. This information is considered 'unsolicited'. An example of 'unsolicited' personal information is where you write to us seeking further information on the services we provide or to provide feedback on your experience with the company and you provide information that is not required to respond to your query or feedback.

We will deal with unsolicited personal information in accordance with the APPs. We will destroy your personal information unless we consider that we could have lawfully collected it under the APPs.

Collection of personal information about children and vulnerable people

We will only collect personal information about children when required or authorised by or under law, or otherwise in accordance with the Privacy Act. Additional safeguards apply to protect vulnerable individuals.

Purposes for which personal information may be collected

We may collect personal information about you for the following purposes:

- employment, work health and safety and personnel matters
- to enable us to provide clinical services to you
- policy development, research, and evaluation of our programs and services
- the management of contracts, funding agreements and procurement processes
- individuals signed up to distribution and mailing lists
- complaints (including privacy complaints) made and feedback provided to us
- the provision of legal advice by internal and external lawyers
- quality improvement and service evaluation
- regulatory compliance and reporting
- public health surveillance and monitoring

6. Remaining anonymous or using a pseudonym

You may wish to remain anonymous or use a pseudonym when you interact with us. When we deal with you anonymously, we do not collect any personal information or identifiers from you. Using a pseudonym means to use a different name or term instead of your actual name.

Where possible, we will allow you to interact with us anonymously or using a pseudonym. For example, we may not need your personal information when you seek general information about a program, policy or consultation process. However, in some circumstances, it may be impracticable to remain anonymous or use a pseudonym, or we may be legally required to deal with you in an identified form.

For example, we may not be able to give you access to your personal information under the Freedom of Information Act 1982 unless we are satisfied that the requested information relates to you. It may also be necessary to collect some personal information from you in order to resolve a complaint that you have made. We will notify you at the time of collection if this is the case.

7. Use and disclosure of your personal information

The purpose for which we collect your personal information is important as it restricts how we can use and disclose your personal information. Unless an exception applies in the Privacy Act, we will:

- only use or disclose your personal information for the purpose for which it was collected, and
- where reasonable to do so, notify you of this purpose at the time of collection, or as soon as practicable after collection.

We will only use or disclose your personal information for another purpose where:

- you have provided consent
- it is required by law
- it is reasonably expected and related to the primary purpose
- it is necessary to prevent serious harm
- it is required for law enforcement purposes

8. Purposes for which we may collect, use or disclose your personal information

There are a number of purposes for which we may collect, use and disclose your personal information, which we describe below. References to use and disclosure of your personal information include references to our employees' and contractors' handling of your personal information. We will only collect, use or disclose your personal information in accordance with the Privacy Act and other legislation we administer.

Recruitment processes and onboarding

Personal information collected about applicants during the recruitment process may be used and disclosed by the department as part of both the recruitment and the onboarding process.

For example, personal information collected during the recruitment process may be disclosed to other Australian Government agencies through the creation, use and sharing of a merit list as well as with recruitment agencies engaged by the company to assist with the recruitment process.

Delivering and evaluating our clinical services

Personal information may be used and disclosed for purposes including delivering our clinical services. For example, where you consent, personal information may be used and disclosed in evaluating the success of our services in specific patient cohorts.

Authorised or required by or under an Australian law or court order

Personal information may be used and disclosed where this is authorised or required by or under an Australian law. These third parties may include contracted service providers, Australian Government agencies and state and territory agencies as well as researchers.

For example, we may disclose personal information to state and territory disciplinary bodies for the purposes of investigations into professional misconduct by health professionals, in accordance with the Health Insurance Act 1973.

9. Data linkage and integration

We may on occasion create new datasets by linking data from different sources including data lawfully collected by us from other health providers.

Data linking may involve de-identified information or your personal information. We will only engage in data linking in accordance with the Privacy Act and other legislation we administer and for purposes including:

- statistical and research purposes
- implementing and evaluating the effectiveness of our programs and services
- compliance purposes
- quality improvement and service monitoring
- public health surveillance

We engage in data linking projects with other partners where our participation is in accordance with the Privacy Act and other relevant legislation. Any data linking activities will:

- use privacy-preserving techniques
- be subject to privacy impact assessments
- include appropriate security controls
- be documented and monitored
- follow best practice data minimisation principles

10. Disclosure of your personal information overseas

We disclose personal information to overseas recipients in limited circumstances. These may include when you give consent, where your personal information is not identifiable, or where disclosure is required or authorised by or under law.

We acknowledge that some third-party service providers we engage may store data overseas. Before sending information overseas or engaging third-party providers with overseas data storage, we will:

- conduct privacy impact assessments
- verify recipient privacy practices
- monitor overseas recipients
- maintain detailed records of transfers

We will only provide your personal information to an overseas recipient in accordance with the Privacy Act.

11. Storage of your personal information

Personal information collected and held by third parties

Personal information may be held by us or by people or organisations acting on our behalf, for example, contracted service providers.

Under the Privacy Act, we are required to take measures to ensure that when your personal information is held by a third party, that the third party complies with the same privacy requirements applicable to us.

We include privacy clauses in our contractual agreements with third parties, including funding agreements, consultancy and services contracts and various other ad-hoc contractual agreements. This is to ensure that the third parties handle personal information in accordance with relevant privacy obligations.

Storage, retention and destruction of personal information

Personal information held by us is stored on electronic media, including our Electronic Medical Records system, Enterprise Data Warehouse, business applications and cloud computing solutions. Personal information may also, on occasion, be held on paper files.

We store and dispose of your personal information in accordance with the Archives Act 1983 and relevant records authorities. For more information, see the National Archives of Australia website.

We will take reasonable steps to destroy or de-identify your personal information if we no longer need it for the purpose for which it was collected, unless required or authorised by or under law or a court/tribunal order to retain the information. When personal information is no longer required to be retained as part of a Commonwealth record, it is destroyed in accordance with the Archives Act 1983.

Data security

Electronic and paper records are protected in accordance with the requirements of the APPs.

We protect your information through:

- multi-factor authentication
- encryption at rest and in transit
- regular security assessments
- mandatory staff privacy training
- incident response procedures
- third-party security assessments
- data minimisation practices

We have controls in place for accessing information appropriate to the type and sensitivity of the information. Access to personal records by staff and contractors is restricted to officers on a 'need to know' basis. We also protect your personal information through steps that include password protection for electronic files, securing paper files in locked cabinets and other access restrictions.

12. Access and correction

We will provide access to any personal information that we hold about you, at your request. You may also request correction of your personal information if it is inaccurate, out of date, incomplete, irrelevant or misleading.

You can request access to documents containing your own personal information by emailing us.

We will take reasonable steps to provide you with access and/or make a correction to your personal information within 30 calendar days, unless we consider there is a sound reason under the Privacy Act or other relevant law to withhold the information, or not make the changes.

For example, we may refuse access to your personal information where the record includes another individual's personal information or where refusal is required or authorised by the FOI Act or any other law.

If we do not provide you with access to your personal information, or refuse to correct your personal information, where reasonable we will:

- provide you with a written notice including the reasons for the refusal
- provide you with information regarding available complaint mechanisms
- at your request, take reasonable steps to associate a statement with the personal information that you believe to be inaccurate, out of date, incomplete, irrelevant or misleading.

Updating your personal information

It is important to tell us if your circumstances change to ensure that the information we hold, use or disclose about you is accurate, up-to-date and complete.

13. The Notifiable Data Breaches Scheme

The Notifiable Data Breach Scheme (the NDB Scheme) in Part IIIC of the Privacy Act commenced on 22 February 2018. In accordance with the NDB Scheme, we investigate and undertake assessments of suspected and actual data breaches, and notify 'eligible data breaches' to the OAIC and affected individuals.

We take seriously and deal promptly with any unauthorised access to, disclosure of, or loss of personal information (data breach). Examples of data breaches include a document

containing personal information being sent to the wrong recipient due to human error, or a failure to remove or redact personal information from a record before disclosing it.

Our data breach response includes:

- 72-hour notification requirement where applicable
- comprehensive risk assessment protocols
- documented containment strategies
- prepared notification templates
- post-incident review processes
- preventive measures
- detailed documentation requirements

14. Complaints

Complaints about the treatment of your personal information

If you believe that we have breached the Privacy Act, the Code or otherwise mishandled your personal information, you can contact us.

Each complaint will be dealt with on a case-by-case basis. All complaints will be investigated by us and you will be advised of the outcome.

All privacy complaints are taken seriously. You should not be victimised or suffer negative treatment if you make a complaint.

Making a privacy complaint

If you believe that we have breached the APPs or mishandled your personal information, you should take the following steps:

1. Contact us: in the first instance, any privacy concern or complaint should be reported directly to us.
2. Submit your concern or complaint in writing: in order to be able to fully investigate your complaint, we would prefer that you make your complaint in writing. The complaint should include information about the claimed privacy breach and your contact details. Please note that if you do not provide sufficient information or if you submit an anonymous complaint, we may not be able to fully investigate and respond to your complaint.
3. Reasonable amount of time: we will acknowledge your concern or complaint upon receipt. This may involve email or telephone correspondence with you. We will also provide you with updates as to our investigation into your privacy complaint, if you provide your contact details. We will try to respond to your privacy concern or complaint as soon as practicable.

We will use the information from your complaint to investigate and seek to resolve the issues you have raised.

We will use the information you provide in your complaint to provide feedback to staff or our business areas. If you are not satisfied with our response, you can complain directly to the OAIC.

The OAIC's details are:

Telephone:1300 363 992
Email: enquiries@oaic.gov.au
Post: GPO Box 5218, Office of the Australian Information Commissioner, Sydney NSW 2001

Please note that the OAIC generally requires that a complaint first be raised with us before the OAIC will investigate.

15. Artificial intelligence systems and your privacy

Clean Slate Clinic utilises artificial intelligence (AI) systems to support our services. This section explains how we protect your privacy when using AI technologies.

AI Data Processing and Analysis

Our AI systems enable us to leverage complex healthcare data to improve patient outcomes and refine our treatment approaches. We may use AI systems to:

• Analyse treatment outcomes and patterns
• Identify potential risk factors
• Monitor treatment progress
• Improve service delivery

We maintain rigorous oversight of all AI implementations to ensure they meet the highest standards of accuracy, fairness, and ethical use. All AI processing is subject to:

• Regular oversight by our Clinical Governance Committee
• Strict quality control measures
• Regular accuracy and bias testing
• Privacy impact assessments
• Clinical safety reviews

AI Decision-Making

AI systems serve as valuable tools to support healthcare professionals but never replace human clinical judgment in critical matters. AI systems are not used to make clinical decisions and all significant decisions are made by qualified healthcare practitioners or operational staff.

AI Data Collection and Use

Our AI systems utilise various data sources to generate insights while maintaining strict protocols for data handling and protection. Our AI systems may process:

- Your health records and treatment information
- App usage and interaction data
- Treatment outcome data
- Behavioural patterns and preferences
- Program engagement metrics

This data is:

- De-identified
- Protected by security measures
- Regularly audited for privacy compliance
- Used only for research or healthcare purposes
- Subject to strict access controls

AI Privacy Safeguards

We implement comprehensive safeguards to protect patient information throughout all AI processes and applications. We protect your privacy in AI systems through:

- De-identification techniques
- Regular privacy impact assessments
- Bias detection and minimisation
- Data minimisation practices
- Regular algorithmic audits
- Secure AI model storage
- Strict access controls
- Regular staff training

Your Rights Regarding AI

We believe in transparency and patient autonomy in all aspects of our AI implementation and usage. You have the right to:

- Know when AI is being used
- Understand how AI affects decisions about you
- Opt out of certain AI processing where clinically appropriate
- Access information about AI processing of your data
- Question or challenge AI-supported decisions
- Have AI errors corrected promptly

AI Security Measures

Our robust security infrastructure ensures that all AI systems and associated data remain protected against unauthorised access or misuse. We protect AI systems and data through:

- Secure model storage and transmission
- Protection against unauthorised access
- Regular security testing and updates
- Monitoring for unusual patterns
- Incident response procedures
- Secure backup systems
- Access logging and auditing

16. Updates to this Policy

This policy was last updated in April 2025. We review this policy annually and may update it to reflect changes in privacy law or our practices. We will notify you of significant changes through our website and direct communication where appropriate.