preciselee

Preciselee Privacy Policy

At Preciselee, we value your privacy and are committed to protecting the personal information you entrust to us. We collect, use, store, and share your information responsibly and transparently, in line with Australian privacy laws and ethical medical practice. This Privacy Policy outlines how we handle your data and the principles we follow to ensure your information is treated with care and respect.

What Personal Information Do We Collect?

The personal information Preciselee collects depends on who you are and how we interact with you. We only collect what is necessary to provide our services, manage our relationship with you, and support our business and administrative operations.

This may include your name, contact details, date of birth, sex, medical and family history, clinical images or samples, government identifiers (e.g., Medicare), payment details, and records of our past interactions with you. In some cases, information such as ancestry or religion may be collected if medically relevant.

You can choose to remain anonymous or use a pseudonym unless it is impractical or we are legally required to identify you. Please note this may limit our ability to provide some services or affect their quality.

How Do We Collect the Information?

Where possible, we collect your information from you directly, through forms, phone calls, emails, written correspondence, or our website. If direct collection is not practical, we may collect information from third parties, particularly when urgent medical care is required and your health may be at risk. These third parties may include healthcare professionals involved in your care, your nominated representative, the My Health Record system (if you have opted in), or relevant government agencies.

By providing your personal information to Preciselee, you consent to its collection, use, and disclosure as outlined in this Policy. In some cases, where it is not reasonable or practical to obtain consent directly from you, a responsible person (such as a partner, family member, carer, or someone with medical power of attorney) may provide consent on your behalf. You are not required to provide personal information to us. However, if the information you provide to us is incomplete or inaccurate, the services we provide to you may be affected.

When you visit our websites, we do not identify you unless you choose to provide your details. We use cookies to collect anonymous usage data (e.g., your browser type or pages visited) to improve site performance. Our websites and emails may contain links to external sites. We are not responsible for the privacy practices of those sites, and you should review their privacy policies separately.

How We Use and Disclose Your Personal Information

We use your personal information primarily to deliver diagnostic services, communicate results, and support your care. We will only use or disclose your information for the purpose it was collected or a related secondary purpose. This includes interpreting tests, coordinating with your healthcare providers or payers, fulfilling regulatory obligations, and maintaining internal quality and audit standards. We may also use or disclose your information if you have given consent, or where required or permitted by law.

In the process of providing services to you or otherwise engaging with you, we may share your personal information with trusted third parties. These may include healthcare providers and clinics, statutory bodies or organisations as required by law, and approved service providers such as IT vendors or debt recovery agents. If you participate in the My Health Record system, we may access or upload relevant health information, if required or requested to do so. You can manage or restrict our access by opting out or adjusting your settings within the My Health Record system.

We may also de-identify and aggregate your data for clinical research, quality improvement, service analytics, or other business activities. We do not and will not disclose de-identified data to third parties for the purpose of sale or other commercial gain. We will not request further consent to share your personal information for the purposes already outlined.

How We Protect Your Personal Information

We take your privacy seriously and use reasonable steps to keep your personal information accurate, secure, and protected from misuse, loss, or unauthorised access.

To safeguard your data, we use physical, technological, and administrative measures. These safeguards are regularly reviewed to maintain a high standard of protection. We retain your information only as long as needed for legal, clinical, or business purposes. When no longer required, we securely destroy or de-identify it. If we discover a data breach that is likely to cause serious harm, we will notify you promptly and advise on any necessary steps.

Access and Correction of Personal Information

You have the right to access the personal information we hold about you. We will provide access unless there is a legal reason to limit or refuse it, such as a serious risk to the health, safety, or the privacy of any individual. To request access, please contact our Privacy Officer. We may need to verify your identity and may charge a reasonable fee for providing this information. For pathology test results, we recommend accessing them through your treating practitioner, who can explain the findings in the context of your individual health.

You also have the right to request corrections if you believe the information we hold about you is inaccurate, incomplete, or outdated. If we agree, we will update it. If we do not agree, you may provide a written statement outlining your requested changes, which we will enclose with your personal information. To make a correction request, please contact our Privacy Officer.

How to Contact Us About Privacy Issues and Complaints

If you have questions, concerns, or complaints about this Policy or how we handle your personal information, please email contact@preciselee.co and address your message to our Privacy Officer. We aim to provide a response within a reasonable timeframe, typically within 21 days. If you are not satisfied with our response, you may contact the Office of the Australian Information Commissioner (OAIC), which has the authority to investigate and make determinations on privacy matters.

Updates to This Privacy Policy

Preciselee may update this Policy from time to time. Any changes take effect as soon as they are published on our website. By continuing to use our services after changes are posted, you agree to the updated terms. If you do not agree with the revised Policy, you should not use our services, including our website.

preciselee

Preciselee Data Security Policy

At Preciselee, we are committed to safeguarding the integrity and confidentiality of personal and sensitive information. To protect our systems and uphold patient and stakeholder trust, we apply a layered approach to data security. Our key security measures:

• Data Classification and Protection

We protect data according to its classification (e.g., patient-identifiable). Security measures are tailored to the potential impact of unauthorised data disclosure, modification, or loss.

• Physical Security

Access to areas where data or systems are stored is limited to authorised personnel. Our facilities are equipped with physical security measures to prevent unauthorised entry or interference.

• Access Control

Access to data and systems is restricted according to role and operational need. User access rights are reviewed regularly to ensure they remain appropriate and are promptly revoked when no longer required.

• Workforce Awareness and Training

We foster a culture where data security is everyone's responsibility. All staff receive training on data protection, privacy, and their individual responsibilities as part of onboarding and ongoing professional development.

• Data Backup and Recovery

We perform regular data backups and maintain documented protocols for recovery. Backups are securely stored and periodically tested to ensure data can be restored if needed.