

HONEYSUCKLE HEALTH PRIVACY POLICY

This Privacy Policy was last updated **April 2026**.

1. Introduction

Honeysuckle Health Pty Ltd respects the privacy rights of our customers and other organisations with whom we interact. We are committed to complying with all applicable privacy laws including the Privacy Act 1988 (Cth), Australian Privacy Principles and applicable State legislation.

Within this Privacy Policy, “we”, “our”, “us” and “Honeysuckle Health” refers to:

1. Honeysuckle Health Pty Ltd, ABN 55637339694.
2. hub.Health, Youly, Stagger, hubPass (trading under Midnight Health Pty Ltd, ABN 13 647 966 738).

This Privacy Policy tells you how Honeysuckle Health handles personal information.

2. Collection of Personal Information

I. What Personal Information Do We Collect?

Personal information means information or opinion that reasonably identifies you as an individual. The types of personal information we collect include your name, contact details and gender.

The types of personal information (including sensitive information) we collect will depend on your relationship and interaction with us. This includes whether you are:

- a Honeysuckle Health customer - name, contact details, gender;
- a youly.com.au, stagger.com.au, hub.health, hubPass or midnighthealth.com.au customer
- an authorised representative of a Honeysuckle Health customer – name and contact details;
- a registered health service provider, in relation to your agreement with us or one of our business partners who we act as an agent on behalf of – we collect name, contact details, specialties, registration, and billing details;

Sensitive information is a subset of personal information that includes your health information (including medical history), genetic information, information about your racial or ethnic origin, political opinion, religious beliefs, sexual orientation and criminal record.

Depending on your relationship with us, the types of sensitive health information that we may collect from you includes details about your medical conditions, treatment, and care. We may

also collect information on your cultural background when this is relevant to your care (e.g. to ensure culturally appropriate practices, and to identify cultural-specific programs that may be available to you). Other sensitive information we may collect, where relevant, include your psychosocial situation, and sexual orientation.

II. How We Collect Your Personal and Sensitive Information

a. Information we collect from you

We collect your personal and/or sensitive information, depending on your relationship and interaction with us. Wherever possible, we will seek to obtain your consent prior to collecting your personal and sensitive health information.

This collection may occur in a variety of ways, including:

1. Through the forms you complete in electronic or hard copy form, on our website or through email, when you enrol for our digital health management programs on the relevant apps or where you provide us with information over the telephone
2. Through the forms you complete in electronic form on our website (including hub.health, Stagger, Youly or hubPass) to request clinical services, prescription or partner pharmacy product
3. Through written communications to us via social media, email, SMS, customer support, online live chat, or through a direct website enquiry
4. Through submission of payment details for paid services with credit cards or Paypal.
5. Through telephone recordings of your interactions with Honeysuckle Health services
6. Through clinical consultations and assessments
7. Through job applications or expressions of employment interest

You may nominate a representative to speak with Honeysuckle Health on your behalf and discuss your personal information and sensitive health information with us. Provided that you and your nominated representative both provide consent, we may collect, use and disclose your personal information and sensitive health information to your nominated representative.

b. Information about Authorised Representatives that we collect from Honeysuckle Health Customers.

We may collect the personal information of nominated representatives. We collect this information in order for us to be able to verify the identity of the nominated representative and communicate with them about a patient's care.

c. Information we collect from third parties

We may collect personal information about you from third parties such as your doctor, treating hospital, health insurer, other health service provider, or My Health Record if it is not reasonable or practicable to collect this information from you, or with your consent. This may also include other people or organisations who might be representing you, or any person assisting or representing us.

d. Publicly available resources

We may also collect your personal information from publicly available sources such as internet search engines and social networking services. When we do so, we ensure that we have a legal basis for using your personal information, such as to enable us to contact you and offer our products and services to you.

e. Information we collect from search engines and applications

Like many companies, we use technology and tools (such as 'cookies') that tell us when a computer or device has visited or accessed our website content. Those tools include services from search engines and other companies that help us to tailor our products and services to better suit our customers and potential customers.

Search engines provide facilities to allow you to indicate your preferences in relation to the use of those tools in connection with computers and other devices controlled or used by you. Our mobile applications may also collect precise location information from your device if you consent to the collection of this information, and we will always respect your preferences including if you choose to withdraw your consent at any time.

We strive to collect personal information directly from you with your knowledge and consent. However, if you do not consent and we do not have your personal information, we may not be able to process your requests or employment application or provide our services to you including providing health management programs, health services or other assistance.

3. Remaining Anonymous

You have the right to remain anonymous or use a pseudonym when interacting with us. However, it may not always be possible for us to provide a service to you if you choose to remain anonymous. For example, we may need to liaise with your health insurer or treatment team when we assess your suitability for a particular healthcare program or service. We will inform you if you are unable to remain anonymous when dealing with us.

4. Purposes for Which we Collect, Hold, and Use Your Personal Information

How we use your personal information depends on our relationship and interaction with you. Below are the main purposes for which we collect and use your information:

- to verify your identity, maintain the security of your account, and assist with account access issues such as forgotten usernames or passwords;
- to assess your eligibility to provide or receive Honeysuckle Health products or services;
- to manage, deliver and administer health services, health management programs or products you participate in, including clinical assessment, treatment, personalised health information, and related support services.
- to assess and process requests for clinical assessments, prescriptions, pharmacy treatments, and related health products or services;
- to exchange information with medical professionals where necessary to facilitate the issuing of prescriptions or the provision of healthcare services;
- to respond to enquiries, requests and other communications you submit to us;
- to process authorised financial transactions;
- to process, confirm, fulfil and communicate with you about orders for products or services;
- to provide advice, information, or support tailored to your needs;
- to communicate with you about products and services, including invitations, offers, and new or existing services that we or our business partners believe may be relevant to you, and to support the development and improvement of our products and services;
- to receive, manage and address medical queries, feedback, complaints, clinical incidents, and adverse events, including preparing and submitting adverse reaction reports to relevant regulatory bodies such as the Therapeutic Goods Administration, where required or permitted by law.

Authorised Representative

Where you act as an authorised representative of a Honeysuckle Health customer, we may use your personal information:

- to verify your identity as the authorised representative for the Honeysuckle Health customer; and
- while collecting, using and disclosing the personal information of the patient whom you represent.

Third Parties / Business Partners

Where you interact with us as a third party or business partner, we may use your personal information:

- to carry out a business or professional relationship we may have with you.

Job Applicant

If you apply for employment with us, we may use your personal information:

- to assess and manage your employment application and to contact you in connection with that application.

Health Service Provider

Where you are a health service provider, we may use your personal information:

- to create and provide access for customers and other third parties to directory services.

Internal Purposes

We also use your personal information for the following internal purposes:

- to evaluate the effectiveness of our health management programs and services, and the products or we provide;
- to prepare internal reports for the purposes of improving our products, services and internal operations;
- to manage complaints, disputes and incidents, and report matters to relevant dispute resolution or oversight bodies;
- to manage, train and develop our employees and representatives;
- to perform quality assurance activities, investigations, and clinical or operational reviews and evaluations;
- to amend or update records, including removing personal information where appropriate; and
- for other everyday business purposes that involve the use of personal information.

Use of technology and automated tools

We may use technology-enabled tools, including analytics and artificial intelligence-based tools, to support service delivery, quality improvement, operational efficiency, and administrative functions.

Any use of such tools is subject to appropriate oversight and governance. We take steps to ensure that tools used to handle personal information are assessed for privacy and security risks, including through privacy impact assessments where required, and are approved in accordance with our internal governance frameworks.

These tools are used to support, and not replace, appropriate human oversight in the delivery of our services.

Legal Basis for Use

We ensure that we have an appropriate legal basis to collect and use your personal information, including where:

- it is necessary for our usual business functions and activities (such as managing our business operations and developing and improving our products and services);
- we have clearly explained a proposed use, and you have provided your consent; and
- we are required or authorised by law to do so, it is in the substantial public interest (for example, to prevent fraud, money laundering or comply with regulatory obligations),
- or where it is necessary to establish, exercise or defend legal rights (such as debt recovery) or whenever courts are acting in their judicial capacity.

Marketing Purposes

Some of our products and services involve direct marketing communications, while others do not use direct marketing and instead involve service-related follow-up communications.

Where we conduct direct marketing:

- we may use your personal information to send you marketing communications about our products or services, or those of selected third parties, where permitted under the Australian Privacy Principles and any applicable consent requirements; and
- you may opt out of receiving electronic marketing communications at any time by using the “unsubscribe” function in our communications or by contacting us directly.

Where direct marketing is **not** conducted:

- we may contact you for follow-up communications related to the service(s) you have received, such as checking outcomes, confirming program completion, offering future support, or seeking feedback.
- these follow-up communications are operational or service-related and are not promotional in nature.
- You may opt out of marketing communications at any time.
You may also request not to receive certain service-related follow-up communications, and we will comply with that request to the extent reasonably practicable.

SMS marketing

Where you provide us with your mobile phone number, and where permitted by law, we may use your personal information to send you **SMS marketing communications** about our products or services. These messages may include information about new or existing products or services, promotions, events, or other updates that may be relevant to you.

SMS marketing messages will only be sent where you have **consented** or where otherwise permitted under applicable laws. Message frequency may vary. Standard message and data rates may apply.

You may opt out of receiving SMS marketing communications at any time by replying **“STOP”** to any SMS message you receive from us, or by contacting us directly using the details set out in this Privacy Policy. Once you opt out, we will not send you further SMS marketing messages.

We take reasonable steps to protect your personal information. However, you acknowledge that SMS communications are not completely secure, and we cannot guarantee the security of information transmitted via SMS. If you have concerns about receiving SMS communications, you may contact us to discuss alternative communication methods.

5. Use and Disclosure of Personal Information

We use and disclose your personal information and sensitive health information to relevant individuals, organisations and other contracted entities as is necessary for us to provide our services to you.

For example, we may disclose your personal information to:

- a person acting on your behalf, including a person authorised by you or to whom you have granted a delegated authority;
- your private health insurer (if applicable);
- your medical specialists, your general practitioner and other allied health specialists;
- service providers that we use to carry out activities on our behalf, for example, auditors, IT
- vendors and third-party sub-contractors delivering services on our behalf
- to others who may be involved in your care, for example, hospital discharge planners;
- where relevant, a third-party purchaser of our business or assets;
- where relevant, local registration boards and professional and industry bodies and associations, or to external dispute resolution bodies; and
- in additional ways you may also agree to.

We may also use and disclose your personal information and sensitive health information to comply with Australian Law or if required by a court or tribunal order.

We may also use and disclose your personal information to the extent that we have another legitimate purpose, such as to manage our business operations or to conduct data analytics to improve our offerings. We may also share with others and disclose de-identified personal information (including aggregated, anonymous or pseudonymised information) for business and marketing purposes.

We may use or disclose your personal information in circumstances where we consider that there is an immediate threat to the health or safety of yourself, our patients, staff or the wider public.

hubPass for Business

If you access our services as a hubPass for Business member, your employer may have access to reporting dashboards that contain **de-identified and aggregated information**. These dashboards summarise workforce-level data such as demographics, health risk trends, and overall use of our services across employees.

This information **cannot be used to identify you personally**. To further protect your privacy, we do not display any health-related data where there are fewer than **10 individual data points**.

6. Security of your Personal Information

We have systems and processes in place to securely store your personal information and sensitive health information. Some of our systems for storing your information include:

- electronic storage through computer systems
- paper records; and
- cloud storage.

We take proactive steps to protect your personal information and sensitive health information from misuse, interference, loss, unauthorised access, modification and disclosure with appropriate safeguards and security measures. The measures that we take include:

- only allowing authorised personnel access to your personal and sensitive health information;
- ensuring our personnel is trained and aware of Privacy Acts, Cyber Security Awareness and Australian and Consumer Laws;
- storing and accessing data in secure systems to protect against unauthorised access or misuse; and

- when engaging third-party service providers, conducting supplier assurance activities and ongoing security assessments to ensure your information is handled responsibly.

Our information security controls are supported by an **ISO/IEC 27001-certified information security management system**, which provides a structured, risk-based approach to protecting information.

Our systems are hosted using infrastructure located in Asia-Pacific public cloud regions and, in normal operating circumstances, this means your data is stored in Australia.

When you share information with us (such as over the internet, or by sending us an email), it is at your own risk, as factors beyond our control include the security of your device and/or the program you use, to communicate with us. If you reasonably believe that there has been unauthorised use or disclosure of your personal information, please contact us using the details set out in this privacy policy.

Our website may contain links or references to other websites not subject to this Privacy Policy. You should check their own privacy policies before providing your personal information.

7. Disclosure to overseas recipients

We may need to provide your personal information and sensitive health information to an overseas service provider in circumstances where technical support is required. In such circumstances, we strictly control and limit how they can access your personal information. We also have contractual measures in place to ensure that the overseas recipient will comply with the Australian Privacy Act and the Australian Privacy Principles.

8. Accessing and correcting your personal information

We use our best endeavours to ensure that the personal information we collect, use, and disclose is accurate. Please let us know if there are any errors, or if there are changes to any of your personal information, such as a change of address.

Under the Australian Privacy Act, we are required to provide you with access to the personal information we hold about you. You are also entitled to make an amendment request if you consider the information, we hold about you is inaccurate or incorrect.

We may require proof of identity before processing your access or correction request. We will respond to your request as soon as we reasonably can, including notifying you if we are unable to provide access (such as when we no longer hold the information) or if we are permitted by the applicable law to refuse access.

Generally, we cannot impose a charge for giving access to your own personal information, unless permitted to do so by an Australian law, Court, or Tribunal order. We may however charge you a reasonable fee for the retrieval costs associated with providing you with access.

9. Privacy Enquiries and Complaints

If you have any questions, concerns, or complaints regarding the way that your personal information has been collected or handled by Honeysuckle Health, please contact our Privacy Officer whose contact details are provided below:

Email: privacy@honeysucklehealth.com.au

Mail: Level 1, 6 Newcomen Street, Newcastle, NSW 2300.

We will establish, in consultation with you, a reasonable process, including time frames provided by applicable laws, for seeking to resolve your complaint.

If you are not satisfied with our response, you can contact or make a complaint to the Office of the Australian Information Commissioner.

Email: enquiries@oaic.gov.au

Telephone: 1300 363 992 (from overseas +61 2 9284 9749)

10. Changes to this Privacy Policy

This Privacy Policy is current at April 2026. We may review and change this Privacy Policy from time to time.

Previous changes:

Version	Month	Change
1.8	April 2026	Section 2 (How we collect information): added references to online live chat and telephone call recordings; clarified that we may collect information from My Health Record (where applicable and authorised). Section 4 (How we use information): added internal purposes relating to complaints/disputes/incidents and quality assurance/investigations/reviews; added a new “Use of technology and automated tools” paragraph; updated marketing section to distinguish between direct marketing (where applicable) and service-related follow-up communications; added SMS marketing information.

		Section 5 (Disclosures): added hubPass for Business dashboard reporting clause (de-identified/aggregated), aligned to Midnight Health wording. Section 6 (Security): added reference to ISO/IEC 27001 certification.
1.7	June 2023	Update email address for Honeysuckle Health.
1.6	February 2023	Update to the list of Security measures taken to protect personal information, and the type of sensitive information we may collect. Add types of Health Service Provider information that we collect.
1.5	July 2021	Update to include digital health programs and apps as ways information is collected.
1.4	April 2021	Update to the language in the Disclosure to overseas recipients
1.3	October 2020	Wording on data storage locations to reflect potential disaster recovery / capacity issue scenarios. Added heading numbering
1.2	September 2020	Update of titles for health programs and applicability of the collection notice
1.1	August 2020	Include information handling procedures related to a nominated representative
1.0	April 2020	Initial version