

CONCORD HEART

Shop 4, 114 Majors Bay Road, Concord NSW 2137

Phone: (02) 9030 0384 | Email: reception@concordheart.com.au | Website: www.concordheart.com.au

PRIVACY POLICY

Last updated: September 2026

1. About this policy

Concord Heart ("we", "us", "our", "the practice") provides cardiology consultations and non-invasive cardiac diagnostic testing, including stress echocardiograms, echocardiograms, ECGs and Holter monitoring. We are committed to protecting the privacy of your personal and health information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). This policy explains what information we collect, why we collect it, how we store and protect it, who we share it with, and how you can access, correct or raise concerns about your information.

For more information about your privacy rights, you can visit the Office of the Australian Information Commissioner (OAIC) website:

www.oaic.gov.au/privacy/australian-privacy-principles

2. What personal information we collect

Depending on the care you need, we may collect:

- identity and contact details (name, date of birth, address, phone, email)
- Medicare, DVA and private health fund details
- emergency contact details
- your regular GP and referring doctor details
- health information, including your medical history, current medications, symptoms, test results (such as ECGs, echocardiograms and Holter monitoring reports), consultation notes and treatment details
- billing and payment information

Health information is treated as "sensitive information" under the Privacy Act 1988 (Cth) and is subject to additional protections regarding how it is collected, used and disclosed.

3. How we collect your information

We usually collect your information directly from you, such as when you complete our patient intake form, speak with our reception staff, or attend a consultation. During some consultations, we also use Heidi Health, an AI clinical scribe, to help collect and draft a record of what is discussed (see Section 6 for more information). We may also collect information from your referring doctor, other treating specialists, hospitals, pathology or imaging providers, and Medicare, DVA or your health fund, where necessary for your care or billing.

Any information collected on paper forms is uploaded to your electronic patient file on the same day it is completed, after which the paper form is securely shredded.

4. Why we collect, use and hold your information

We collect, use and hold your personal and health information to:

- provide you with cardiology consultations and non-invasive cardiac diagnostic testing (such as stress echocardiograms, echocardiograms, ECGs and Holter monitoring)
- manage appointments and communicate with you, including reminders
- process Medicare, DVA and private health fund claims and other billing
- coordinate your care with other treating healthcare providers
- meet our legal, professional and regulatory obligations

If you do not provide the information we request, we may be unable to properly assess or treat you, process your claims, or contact you in an emergency.

5. How we store and protect your information

We take the security of your personal and health information seriously. Your information is stored using the following systems, each of which is accessible only to authorised staff and protected by multi-factor authentication (MFA):

- Gentu — our practice management system, used to store and manage your patient file, appointments and clinical records.
- Heidi Health — used to assist with scribing (note-taking) during patient consultations.
- Piccolo Health — used for reporting on cardiac testing performed on the day of your visit.

Access to these systems is restricted to staff who need the information to perform their role. Paper forms are shredded on the day they are completed, once the information has been uploaded to your electronic patient file. We regularly review our security practices to protect your information from misuse, interference, loss, and unauthorised access, modification or disclosure.

Retention and destruction of your information

In accordance with the Health Records and Information Privacy Act 2002 (NSW), we retain patient health records for a minimum of seven years from the date of your last consultation, or until you turn 25 years of age if you were a minor when treated, whichever is longer. Once this retention period has passed and the information is no longer required, records are securely destroyed or de-identified.

6. Automated decision-making and AI-assisted tools

We use Heidi Health, an AI-powered clinical documentation assistant, during some consultations to help your doctor prepare clinical notes.

- Type of tool: Heidi Health, an AI clinical scribe used during patient consultations. It is the only AI tool we use, and only your treating doctor has access to their own Heidi Health account.
- What it does: Heidi listens to, or processes a transcript of, your consultation to prepare a draft clinical note and, where relevant, a draft consultation letter. It does not diagnose, treat or make any clinical decision — your doctor reviews, edits and approves all content before it becomes part of your record or is sent to your referring doctor or other treating providers.
- What information it accesses: the personal and health information discussed during your consultation, such as your symptoms, medical history and your doctor's observations.

Your information is used by Heidi Health solely to prepare your consultation note and letter. It is not used to train Heidi Health's underlying AI models, and is not shared with, or used by, any other AI tool or platform. Your doctor will confirm your consent to use Heidi Health verbally at the start of your consultation, and you may decline or withdraw this consent at any time without affecting your care. Once your consultation letter has been finalised and sent, the recording, transcript and draft notes held within Heidi Health are deleted.

Heidi Health's transcript is a machine-generated draft and may not always be a fully accurate record of your consultation, so we do not provide patients with a copy of it. Your doctor reviews the transcript and finalises the relevant content into your consultation letter, which forms part of your medical record and which you may request a copy of at any time in line with Section 9 (Access and correction). Once the transcript has been used to prepare your letter, it is deleted. Prior to its deletion, the transcript is not accessible to anyone other than your treating doctor.

For more information about how Heidi Health handles personal information, including its own privacy policy and consent information, please visit:

www.heidihealth.com

7. Who we share your information with

We may share relevant information, only where necessary for your care or as required by law, with:

- your referring doctor and regular GP
- other specialists, pathology and imaging providers involved in your care
- hospitals or other specialist clinics involved in your care, including at their request for treatment purposes
- Medicare, the Department of Veterans' Affairs (DVA) and your private health fund, for billing and claiming purposes

We do not sell your personal information, and we do not disclose it to any other third party without your consent unless required or authorised by law.

8. Overseas disclosure

We do not disclose your personal information to recipients located overseas. The systems we use to store and manage your information (Gentu, Heidi Health and Piccolo Health) are operated on this basis. If this changes, we will update this policy accordingly.

9. Access and correction

You may request access to, or correction of, the personal and health information we hold about you at any time by contacting our reception staff. We will respond to your request within a reasonable timeframe. In some circumstances, access may be limited in accordance with the Privacy Act — if this occurs, we will explain the reason.

Requests for access or correction can be directed to our Practice Manager:

- Practice Manager, Concord Heart
- Phone: (02) 9030 0384
- Email: reception@concordheart.com.au

10. Complaints

If you have a concern about how we have handled your personal information, please contact our Practice Manager in the first instance, using the details above. Where possible, complaints should be made in writing so we can properly investigate the matter. We will acknowledge your complaint and aim to respond within a reasonable time, usually within 30 days.

If you are not satisfied with our response, you may contact the OAIC:

- Phone: 1300 363 992
- Website: www.oaic.gov.au

11. Data breaches

In the unlikely event of a data breach that is likely to result in serious harm, we will comply with our obligations under the Notifiable Data Breaches scheme, including notifying affected individuals and the OAIC where required.

12. Changes to this policy

We may update this policy from time to time to reflect changes in our practices or legal obligations. The current version will always be available on our website and from our reception staff.

13. Accessing this policy

This policy is available free of charge on our website, or you can collect a copy at one of our practice locations.

14. Contact us

If you have any questions about this policy or how we handle your information, please contact us:

- Phone: (02) 9030 0384
- Email: reception@concordheart.com.au