



Heart of Canberra — Privacy policy

DR KASHIF KALAM · MBBS, FRACP · CARDIOLOGIST

Address Suite 8, 12 Napier Close, Deakin ACT 2600 **Phone** 02 6162 2741 **Email** admin@heartofcanberra.com.au

Web www.heartofcanberra.com.au

VERSION 1.0 — 2 September 2026

PRIVACY OFFICER The Practice Manager

REVIEW BY 2 September 2027

ABOUT THIS POLICY

Heart of Canberra is the private cardiology practice of Dr Kashif Kalam at Suite 8, 12 Napier Close, Deakin ACT 2600. This policy explains how the practice collects, uses, stores, shares and protects your personal information, including your health information, and how you can access it, correct it or complain.

The practice is bound by the Privacy Act 1988 (Cth) and the Australian Privacy Principles, and, because the rooms are in the Australian Capital Territory, by the Health Records (Privacy and Access) Act 1997 (ACT). Where the two set different standards, the practice follows the stricter one.

This policy covers patients, people enquiring about care, referring and treating doctors, and anyone else whose personal information the practice holds. The website has its own, shorter privacy statement covering analytics, cookies and the online forms; it is at heartofcanberra.com.au/privacy.

WHAT WE COLLECT

Only what is needed to provide safe care, communicate with your other doctors, and meet legal and billing obligations. Typically that includes:

- Your name, date of birth, sex, address, phone numbers, email and preferred way to be contacted.
- Medicare, DVA and concession card details, and private health fund details if you give them.
- Your referring doctor, your usual GP and other treating doctors.
- An emergency contact and, if you nominate one, a carer or support person.
- Health information: your symptoms and history, medications and allergies, examination findings, and the results, images and recordings of investigations performed here — ECGs, echocardiograms, stress tests, rhythm and blood pressure monitoring, and pacemaker checks.
- Reports and correspondence from other providers — pathology, radiology (including cardiac CT and MRI performed at partner practices), hospitals and specialists.
- Family history and, where relevant to your care, genetic information.
- Billing and payment records.
- Whether you identify as Aboriginal or Torres Strait Islander, if you choose to tell us, so the practice can offer the right services.

Health information is sensitive information under the Privacy Act. The practice collects it only with your consent, or where the law allows collection without it — for example to lessen a serious threat to life or health.

HOW WE COLLECT IT

- Directly from you — on the new patient registration form, in consultations, by phone, and through the website forms.
- From your referring doctor and other treating providers, in the referral and in results and reports sent to the practice.
- From Medicare and DVA, to confirm eligibility and process claims.
- From a person you have authorised to act for you, such as a carer, guardian or attorney.

The practice participates in My Health Record. Where it helps your care, and unless you have asked us not to, the practice may view your My Health Record and may upload documents such as event summaries or reports to it. Not every document is uploaded. You control your own record, including who can see it, through myGov, and you can tell the practice at any time not to upload.

You may deal with the practice anonymously or under a pseudonym for a general enquiry. It is not possible for clinical care, Medicare billing or a referral, where the practice must know who you are.

WHY WE COLLECT, HOLD AND USE IT

- To assess, investigate and treat you, and to keep an accurate clinical record.
- To communicate with your referring doctor, your GP and the rest of your treating team.
- To arrange investigations elsewhere, such as cardiac CT or MRI at a radiology practice, and to receive the results.
- To bill you, Medicare, DVA or your health fund, and to manage accounts.
- To send appointment reminders and results correspondence by the channel you have chosen.
- To meet legal and professional obligations — mandatory reporting, responding to a subpoena or court order, Medicare and AHPRA requirements, accreditation and quality activities.
- To manage complaints, claims and incidents, including with the practice's insurer and legal advisers.

The practice does not use your information for research or teaching, does not use it for direct marketing, and does not sell it.

WHO WE SHARE IT WITH

Your information is shared only for the purposes above, or with your consent, or where the law requires or allows it.

Recipients may include:

- Your referring doctor and GP, who receive a report after each consultation and investigation. You can ask for this to be limited, and the practice will explain any consequences for your care.
- Other treating doctors, allied health providers and hospitals involved in your care, including in an emergency.
- Pathology and radiology practices that perform investigations the practice requests.
- Medicare, DVA and private health funds, for claims and eligibility.
- Secure messaging and IT providers that carry or store the practice's records under contract and confidentiality obligations — for example HealthLink for encrypted referrals and reports.
- The practice's professional advisers, insurer and regulators, where required.
- Anyone the law compels the practice to tell, such as a court, or where disclosure is necessary to lessen a serious threat to life, health or safety.

Your clinical and billing records are kept in Genie, the practice management and clinical software supplied by Magentus, under a contract that binds the supplier to confidentiality and security obligations. The records are stored in Australia.

If an account remains unpaid after reasonable reminders, the practice may refer it to a debt collection agency. Only the information needed to recover the debt — your name, contact details and the amount owed — is provided; no clinical information is disclosed.

OVERSEAS DISCLOSURE

Your health records are held in Australia. The practice does not send patient information overseas, and none of the software, backup or support providers it uses stores or accesses patient information outside Australia.

The website uses analytics services with servers outside Australia; they do not receive health information. The website privacy statement describes them.

HOW WE STORE AND PROTECT IT

- Clinical records are kept electronically, with individual staff logins, role-based access and audit trails. Paper received from elsewhere is scanned into the record and the original securely destroyed or filed.
- All staff and contractors are bound by confidentiality obligations and trained in privacy.
- Records and correspondence are transmitted by encrypted secure messaging wherever the recipient supports it. Fax and email are used where they do not, in line with the practice's procedures.
- Systems are backed up, patched and protected against unauthorised access.

Records are retained for at least as long as the ACT Health Records (Privacy and Access) Act requires: seven years from the last time you received a service from the practice, or, if you were under 18 when the record was made, until you turn 25. Records are then securely destroyed and an entry made in the practice's disposal register.

If a data breach occurs that is likely to result in serious harm, the practice will notify the Office of the Australian Information Commissioner and the people affected, as the Notifiable Data Breaches scheme requires.

ACCESS AND CORRECTION

You can ask to see or receive a copy of your health record, or to have it explained to you by a doctor. Requests go to the privacy officer, in writing where possible, and the practice will need to confirm your identity. Under ACT law the practice will respond within two weeks. A reasonable fee may be charged for copying or a written summary, and you will be told what it is before any cost is incurred; there is no fee for making the request.

Access can be refused only in the limited circumstances the law allows — for example where it would pose a serious threat to someone's life or health, or affect another person's privacy — and the practice will explain the reason.

If you believe information the practice holds is inaccurate, incomplete or out of date, ask for it to be corrected. The practice will correct it, or, if it disagrees, attach a statement of your view to the record.

Someone else can access your record on your behalf if you have authorised them, or if they are your legal guardian or attorney, subject to the same checks.

REMINDERS AND HOW WE CONTACT YOU

With your agreement, the practice sends appointment reminders and follow-up messages by SMS or email, and phones you about results that need discussion. Tell reception at any time to change how you are contacted, or to stop reminders.

QUESTIONS AND COMPLAINTS

Contact the privacy officer at the rooms — by phone, email or letter to the address above — with any question about this policy, or if you believe the practice has mishandled your information. The practice will acknowledge a complaint promptly, investigate it, and respond in writing within 30 days.

If you are not satisfied with the response, you can complain to the Office of the Australian Information Commissioner (oaic.gov.au, 1300 363 992) or, for health records in the ACT, to the ACT Human Rights Commission's Health Services Commissioner (hrc.act.gov.au).

CHANGES TO THIS POLICY

This policy is reviewed at least once a year and whenever the practice's systems or the law change. The current version is available on the website, at the rooms, and on request. Continuing to use the practice's services after a change means the updated policy applies.

This policy is available free of charge on the practice website, at the rooms, and on request in another format.