

# PRIVACY POLICY

Last updated: April 2026 | Effective date: April 2026

Coda Crimson Pty Limited A.C.N. 696 491 488 ("Coda Crimson", "we", "us", or "our") is committed to protecting the privacy and confidentiality of personal information, including health information, in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), and the Notifiable Data Breaches (NDB) Scheme.

This Privacy Policy describes how we collect, use, disclose, and manage personal information through our Chronic Disease Management Platform (the "Platform") provided to healthcare organisations ("Clients").

## 1. ABOUT THIS POLICY

This policy applies to all personal information and health information collected and processed by Coda Crimson through its Platform. By using our Platform, Clients acknowledge they have read and understood this Privacy Policy.

Coda Crimson operates as a data processor on behalf of its Clients, who are the data controllers of the personal information and health information entered into the Platform. Clients are responsible for ensuring their own compliance with applicable privacy laws.

## 2. INFORMATION WE COLLECT

### 2.1 Information collected from Clients (B2B)

We collect the following information from healthcare organisations that use our Platform:

- Business contact details (name, email, phone, address)
- Billing and payment information
- Platform usage data and access logs
- Technical data including IP addresses and browser information

### 2.2 Health information processed on behalf of Clients

Our Platform may process health information entered by Clients about their patients, including:

- Patient demographic information
- Medical records and clinical notes
- Appointment and scheduling data
- Treatment and billing records

This health information is processed on behalf of our Clients. Coda Crimson does not own, control, or use this health information for any purpose other than providing the Platform services.

## 3. HOW WE USE PERSONAL INFORMATION

We use personal information collected from Clients to:

- Provide, maintain, and improve the Platform
- Process billing and payments

- Provide technical support and customer service
- Send service-related communications
- Comply with legal and regulatory obligations
- Ensure the security of the Platform

We will not use personal information for any purpose not stated in this Privacy Policy without your prior consent.

#### **4. DISCLOSURE OF PERSONAL INFORMATION**

We may disclose personal information to:

- Our contracted service providers (including AWS cloud infrastructure) who assist in delivering the Platform, under strict confidentiality obligations
- Professional advisers including lawyers and accountants, under confidentiality obligations
- Regulatory bodies or law enforcement agencies where required by law

We do not sell, rent, or trade personal information to third parties.

Where we disclose personal information to overseas recipients (including cloud service providers), we take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information, in accordance with APP 8.

#### **5. HEALTH INFORMATION**

Health information is treated as sensitive information under the Privacy Act 1988 (Cth) and is afforded a higher level of protection. We:

- Store all health information on AWS servers located in Australia (ap-southeast-2, Sydney)
- Encrypt health information in transit and at rest
- Restrict access to health information to authorised personnel only
- Do not use health information for any secondary purpose without consent
- Comply with the requirements of the Privacy Act 1988 (Cth) regarding health information

#### **6. DATA SECURITY**

We implement appropriate technical and organisational measures to protect personal information against unauthorised access, disclosure, alteration, or destruction, including:

- Encryption of data in transit (TLS) and at rest (AES-256)
- Access controls and multi-factor authentication
- Regular vulnerability scanning and security assessments
- ISO/IEC 27001:2022 certified cloud infrastructure (AWS)
- Employee and contractor confidentiality agreements and security training

#### **7. DATA RETENTION**

We retain personal information only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. When personal information is no longer required, we securely delete or de-identify it in accordance with our Data Management Policy.

#### **8. ACCESS AND CORRECTION**

Clients and individuals have the right to access personal information we hold about them and to request corrections. To make a request, please contact us at the details below. We will respond within 30 days of receiving a request.

We may decline access or correction requests in limited circumstances permitted by the Privacy Act 1988 (Cth), and will provide reasons for any refusal.

## **9. NOTIFIABLE DATA BREACHES**

In the event of an eligible data breach under the Notifiable Data Breaches (NDB) Scheme, we will:

- Notify the Office of the Australian Information Commissioner (OAIC) as soon as practicable
- Notify affected individuals where required
- Take immediate steps to contain and remediate the breach

## **10. COMPLAINTS**

If you have a complaint about how we have handled your personal information, please contact us in the first instance. If you are not satisfied with our response, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC) at [www.oaic.gov.au](http://www.oaic.gov.au) or on 1300 363 992.

## **11. CONTACT US**

For privacy-related enquiries, please contact:

**Privacy Officer**

Coda Crimson Pty Limited  
Sydney, New South Wales, Australia  
Email: [info@codacrimson.com.au](mailto:info@codacrimson.com.au)

## **12. CHANGES TO THIS POLICY**

We may update this Privacy Policy from time to time. We will notify Clients of material changes via email or through the Platform. Continued use of the Platform after notification constitutes acceptance of the updated policy.