Clinically

Privacy Policy

Policy

Code: PRV-001

Version: 1

Effective Date: 03 Mar 2026

Review Date: 03 Mar 2027

Author: Wojt Janowski

Approved By: Wojt Janowski (03 Mar 2026)

Owner: Wojt Janowski

This policy complies with: Australian Privacy Principles; SOC 2; ISO 27001; My Health Records Act 2012; Healthcare Identifiers Act 2010

1. About This Policy

CCMx Pty Limited (ABN 24 693 129 056) ("Clinically", "we", "us", "our") provides a cloud-based clinical workflow management platform to Australian healthcare providers. Our platform helps healthcare practices manage referrals, patient records, clinical documents, practice communications, and appointment scheduling.

This Privacy Policy explains how we collect, use, store, disclose, and protect personal information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). It covers personal information we process in our capacity as both a data processor (on behalf of healthcare organisations that use our platform) and as a business in our own right (for our direct customers and website visitors).

We are committed to protecting the privacy and security of health information entrusted to our platform.

2. Who This Policy Applies To

This policy is relevant to:

- **Patients** whose information is managed by a healthcare practice using our platform. Your healthcare provider is the primary holder of your health information — we process it on their behalf.
- **Healthcare practitioners and practice staff** who use the platform as registered users.
- **Referring practitioners** whose professional details are stored in connection with patient referrals.
- **Website visitors and prospective customers** who interact with our website or enquire about our services.

3. Our Role: Processor vs Controller

It is important to understand the distinction between our role and the role of the healthcare practices that use our platform:

- **Your healthcare provider** (the practice using Clinically) decides what patient information to collect, why it is collected, and how it is used. They are the APP entity with primary obligations to you under the Privacy Act.
- **Clinically** provides the technology platform that stores and processes this information on the practice's behalf. We act as a data processor and do not independently decide how patient information is used.

If you have questions about how your health information is used, your first point of contact should be your healthcare provider. If you have questions about how we protect information on our platform, please contact us using the details in Section 13.

4. Information We Collect and Process

4.1 Information processed on behalf of healthcare practices

When a healthcare practice uses our platform, the following personal information may be processed and stored on our systems at the direction of the practice:

Category	Examples
Patient demographics	Name, date of birth, gender, addresses, phone numbers, email
Government identifiers	Medicare number, DVA number, Individual Healthcare Identifier (IHI)
Health information	Clinical documents, referrals, pathology and radiology results, clinical notes, triage data
Communications	Email, SMS, and fax messages between the practice and patients or referrers
Appointments	Appointment dates, types, waitlist entries, check-in records
Form submissions	Patient intake forms, questionnaires, and consent forms completed online
Referrer details	Referring practitioner names, provider numbers, clinic contact details

4.2 Information we collect directly

We collect the following information in our own capacity:

- **Account information:** Practice name, ABN, administrator name and email, user names and emails, role assignments.
- **Billing information:** Payment processing is handled by a PCI-compliant third-party provider. We store your subscription details but do not store credit card numbers on our

systems.

- **Usage and technical data:** Session data, IP addresses, browser type, activity logs for security monitoring. This information is used to protect accounts and investigate security incidents.
- **Website enquiries:** Name, email, phone number, and message content submitted through our website contact forms.

5. How We Use Information

We use personal information only for the following purposes:

- **Providing the platform:** Storing, processing, and displaying patient records, clinical documents, communications, and appointments as directed by the healthcare practice.
- **AI-assisted document processing:** Incoming clinical documents (such as referrals and pathology results) are analysed using artificial intelligence to classify document types and extract patient details. This helps practices process incoming correspondence more efficiently. See Section 7 for details.
- **Communication delivery:** Sending emails, SMS messages, and faxes on behalf of practices to patients and referrers.
- **Security and integrity:** Detecting and preventing unauthorised access, fraud, and security threats. This includes session monitoring, login attempt tracking, and audit logging.
- **Platform operation:** System monitoring, backup and disaster recovery, performance optimisation, and technical support.
- **Billing and account management:** Managing subscriptions, processing payments, and communicating with practice administrators about their account.

We do not use patient health information for marketing, advertising, research, or any purpose other than providing the platform services to the healthcare practice.

6. How We Protect Information

We take the security of health information seriously. Our platform implements the following protections:

6.1 Encryption

- **Files at rest:** All clinical documents and attachments are encrypted at rest using industry-standard authenticated encryption. Each healthcare practice has its own unique encryption keys, so a compromise of one practice's keys cannot affect another.

- **Sensitive database fields:** Medicare numbers, DVA numbers, Individual Healthcare Identifiers, and dates of birth are individually encrypted in the database.
- **Data in transit:** All connections between your browser and our servers, and between our servers and databases, are encrypted. We enforce HTTPS on all traffic.
- **Backups:** Database backups are encrypted at rest.

6.2 Tenant Isolation

Each healthcare practice on our platform receives a completely separate database. Patient data from one practice is physically isolated from all other practices. This means a security incident affecting one practice's data cannot expose another practice's patients. User sessions are also stored within each practice's isolated database.

6.3 Access Controls

- **Authentication:** We support passwords, single sign-on, passkeys, and two-factor authentication. Practices can enforce security policies such as mandatory two-factor authentication.
- **Authorisation:** Role-based access controls ensure users only see what they need for their role within the practice.
- **Session security:** Sessions are monitored for suspicious activity including concurrent logins, unusual locations, and session hijacking attempts.

6.4 Monitoring and Audit

Security events (logins, permission changes, data access, policy enforcement) are logged with a 365-day retention period. We monitor for failed login attempts, unusual session activity, and other security indicators.

7. Artificial Intelligence and Automated Processing

Our platform uses AI to help healthcare practices process incoming clinical documents more efficiently. We believe in being transparent about this.

7.1 What AI is used for

- **Document classification:** When a clinical document arrives (via email or fax), AI analyses the document text to determine its type — for example, whether it is a referral, pathology result, or radiology report.
- **Patient data extraction:** AI extracts patient details (name, date of birth, Medicare number) from incoming documents to match them with existing patient records or assist

in creating new records.

- **Conversation summaries:** When a communication thread is resolved, AI may generate a brief one-sentence summary to help the practice track correspondence.
- **Form translation:** AI translates form labels and instructions into other languages. This processes the form structure, not patient-submitted data.

7.2 How we handle AI processing

- AI processing is performed using infrastructure hosted in Australian data centres. Patient data does not leave Australian jurisdiction for AI processing.
- Our AI provider does not use patient data to train or improve its models, and does not retain prompts or responses after processing is complete.
- AI is used to assist practice staff, not to make clinical decisions. All AI outputs (document classifications, extracted data) are presented for human review.
- AI processing is logged in the practice's database for auditability.
- We are actively working to minimise the amount of patient-identifiable information included in AI processing where identification is not required for the task.

8. Where We Store Information

All platform data is stored within data centres located in Sydney, Australia. This includes databases, file storage, backups, search indexes, and AI processing.

Our platform infrastructure and ancillary services are hosted and operated as follows:

Service Category	What It Does	Data Location
Cloud infrastructure	Primary hosting: databases, file storage, email processing, AI processing, backups	Australia (Sydney region)
DDoS protection and content delivery	Protects the platform from cyberattacks. Data transits through global edge servers but is not persistently stored.	Global (transient only)
SMS and fax delivery	Delivers SMS messages and faxes to patients and referrers on behalf of practices	Australia
Email delivery	Delivers outbound emails from the practice inbox	Australia

Payment processing	Subscription billing and payment processing. No patient data is sent to this provider.	United States (billing data only)

We maintain a detailed register of all sub-processors, including specific provider names and their data handling practices. This register is available on request to healthcare practices and during procurement due diligence.

9. When We Disclose Information

We disclose personal information only in the following circumstances:

- **To provide the service:** To sub-processors listed in Section 8, to the extent necessary to operate the platform (e.g., sending an SMS requires sharing the patient's phone number with our SMS provider).
- **At the practice's direction:** Healthcare practices may configure integrations (e.g., EMR synchronisation, automation webhooks) that involve sharing patient data with external systems. These are configured and controlled by the practice.
- **Legal requirements:** If required by law, court order, or regulatory authority. We will notify the affected practice unless prohibited from doing so.
- **Data breach notification:** If we become aware of an eligible data breach under the Notifiable Data Breaches scheme, we will notify the Office of the Australian Information Commissioner (OAIC) and affected individuals as required by Part IIIC of the Privacy Act.

We do not sell personal information. We do not share patient information with advertisers or marketing services.

10. Data Retention

Patient health information is retained on our platform for the duration of the healthcare practice's subscription. We do not independently delete patient records during an active subscription — the practice manages their own records through the platform.

Healthcare record retention obligations: Australian state and territory legislation generally requires healthcare providers to retain clinical records for a minimum of 7 years from the date of last contact for adult patients, and until a minor patient reaches 25 years of age (or 7 years from last contact, whichever is longer). These are obligations on the healthcare practice, not on Clinically. Our platform supports these obligations by retaining data for the duration of the tenancy.

When a practice leaves Clinically: Upon account closure, we will make the practice's data available for export for 30 days. After the export period, all data associated with the practice

(databases, encrypted files, and backups) will be permanently destroyed within our backup lifecycle, which is a maximum of 180 days from the date of account closure.

Security and audit logs: Activity logs are retained for 365 days within each practice's database to support security monitoring and incident investigation.

11. Your Rights

11.1 For patients

Your healthcare provider is the primary holder of your health information. Under the Australian Privacy Principles, you have the right to:

- **Access** the personal information held about you (APP 12). Contact your healthcare provider to request access to your records.
- **Request correction** of personal information that is inaccurate, out of date, incomplete, or misleading (APP 13). Contact your healthcare provider to request a correction.

If your healthcare provider uses our platform, they can access and export your records through our administrative tools. We will assist practices in responding to access and correction requests.

11.2 For healthcare practices (platform users)

As a practice using our platform, you can:

- Access, update, and manage all patient records and practice data through the platform interface.
- Export patient records to fulfil access requests from patients.
- Configure security policies (two-factor authentication, SSO requirements) for your users.
- Request account closure and data destruction as described in Section 10.

12. Complaints

If you believe we have breached the Australian Privacy Principles, you can lodge a complaint with us using the contact details in Section 13. We will acknowledge your complaint within 5 business days and aim to resolve it within 30 business days.

If you are not satisfied with our response, you may lodge a complaint with the Office of the Australian Information Commissioner (OAIC):

- Online: www.oaic.gov.au/privacy/privacy-complaints

- Phone: 1300 363 992
- Post: GPO Box 5218, Sydney NSW 2001

13. Contact Us

For privacy-related enquiries or to make a complaint:

Email: hello@clinically.com.au

Post: Suite 2 710 Hunter Street Newcastle West NSW 2302

We will respond to privacy enquiries within 5 business days.

14. Changes to This Policy

We may update this policy from time to time to reflect changes in our practices, technology, or legal requirements. When we make material changes, we will notify affected practices via email and update the "Last updated" date at the top of this policy.

We encourage you to review this policy periodically.

Change History

Version	Date	Author	Change Summary
1	03 Mar 2026	Wojt Janowski	Replaced hardcoded "Clinically Pty Ltd (ABN [TBC])" with {{org.legal_name}} and {{org.abn}} placeholders. Also replaced contact details with {{org.contact_email}} and {{org.address}} placeholders.