Clinically

Privacy Policy - Mobile App

Policy

Code: PRV-004

Version: 1

Effective Date: 22 Mar 2026

Review Date: 22 Mar 2027

Author: Wojt Janowski

Approved By: Wojt Janowski (22 Mar 2026)

Owner: Wojt Janowski

Clinically Mobile App — Privacy Policy

Effective Date: 23 March 2026 **Version:** 1.0 **Publisher:** CCMx Pty Limited (ABN 24 693 129 056), trading as Clinically

---

1. About This Policy

This privacy policy applies specifically to the Clinically mobile application ("the App") available on the Apple App Store and Google Play Store. It supplements the Clinically Platform Privacy Policy and should be read alongside it.

The App is designed exclusively for use by healthcare professionals (doctors, specialists, and clinical staff) as a companion to the Clinically cloud platform. It is not intended for patients. No patient-facing features are provided.

2. Who We Are

CCMx Pty Limited (ABN 24 693 129 056), trading as Clinically, operates the App and the underlying cloud platform.

- **Email:** hello@clinically.com.au
- **Phone:** +61 2 4092 7710
- **Address:** Suite 2, 710 Hunter Street, Newcastle West NSW 2302, Australia

3. Data We Collect and Why

3.1 Account and Authentication Data

Data	Purpose	Storage
Email address and name	Identify the authenticated clinician	Encrypted on-device secure storage (iOS Keychain / Android Keystore)
Authentication token	Maintain your session with the Clinically API	Encrypted on-device secure storage
Tenant (practice) identifier	Connect you to your healthcare practice	Encrypted on-device secure storage

Lock PIN hash	Optional app-lock for additional device security	Encrypted on-device secure storage

3.2 Clinical Data (Processed on Behalf of Your Practice)

The App displays clinical data retrieved from the Clinically platform, including:

- Patient names, dates of birth, and demographics
- Clinical documents (including PDFs)
- Triage referrals and associated clinical information
- Tasks and workflow items
- Document comments entered by clinicians

Your healthcare practice is the data controller. Clinically processes this data on behalf of your practice under its service agreement. We do not use clinical data for any purpose other than providing the App's functionality to you.

On-device caching: API responses are encrypted using AES-256 and cached in a local database with short time-to-live periods (2-10 minutes depending on data type) to enable offline access and improve responsiveness. Clinical documents (PDFs) are stored temporarily on-device for viewing. Cached data and temporary files are cleared on logout.

3.3 Device Permissions

The App requests the following device permissions. Each is used solely for the stated purpose and can be revoked at any time through your device settings.

Permission	Why We Need It
Camera	Capture images for clinical workflows (e.g. photographing documents or wound images for records).
Barcode/QR Scanner	Scan barcodes and QR codes for quick patient or document lookup.
Location	Automatically identify which hospital or clinic you are currently at to streamline ward round workflows. Location data is sent to the Clinically API for facility matching and is not stored persistently on-device or used for tracking. We do not store or log your location data in the app or on the Clinically platform.

Microphone	On-device speech-to-text transcription for clinical note dictation.
Background Microphone	Continue dictation transcription when the device screen is asleep during consultations.
Biometric Authentication	Verify your identity locally using Face ID, Touch ID, or Android biometric APIs for app unlock. Biometric data never leaves your device and is managed entirely by the operating system.
Push Notifications	Receive timely alerts about new triages, clinical documents, and tasks. Notifications may include patient names to help you prioritise urgent items. Delivered via Firebase Cloud Messaging (see Section 4).
Storage (Read/Write)	Read and write files required by the App such as downloaded clinical documents and the speech-to-text model.
Network State	Detect connectivity to queue actions for later submission when offline.
Vibration	Provide haptic feedback for interactions and notifications.

3.4 On-Device Speech-to-Text

The App includes an on-device speech-to-text engine (based on OpenAI Whisper) that runs entirely on your device.

- **No audio is transmitted off-device.** All speech recognition processing occurs locally.
- A machine learning model (~142 MB) is downloaded to your device on first use.
- Transcribed text is displayed in the App for you to review and edit before saving.
- Transcribed text is only sent to the Clinically API when you explicitly save it (e.g. as a document comment).

3.5 Error Monitoring and Performance Data

We use **Sentry** (provided by Functional Software, Inc.) to monitor application errors and performance. Sentry collects:

- Error and crash reports (stack traces, exception messages)
- Performance traces (page load times, API response times, database query durations)
- Device metadata (operating system, app version, device model)

- Breadcrumbs (navigation events, UI interactions leading up to an error)

Sentry does not collect patient data, clinical content, or personally identifiable health information. Error reports may include your anonymised session identifier for debugging purposes.

Sentry data is processed in accordance with Sentry's Privacy Policy and is used solely to identify and fix bugs, improve reliability, and monitor App performance.

4. Third-Party Services

Service	Provider	Purpose	Data Sent
Firebase Cloud Messaging (FCM)	Google LLC	Push notification delivery	Device push token, notification payload (may include patient names)
Sentry	Functional Software, Inc.	Error monitoring and performance tracing	Crash reports, performance metrics, device metadata (see Section 3.5)

No other third-party SDKs, analytics services, or advertising frameworks are included in the App. We do not sell, rent, or share your data with third parties for marketing or advertising purposes.

5. Data Storage and Security

5.1 On-Device

- Authentication credentials are stored in platform-provided secure storage (iOS Keychain / Android Keystore), encrypted by the operating system.
- Cached API responses are encrypted using AES-256 before being written to the local database.
- Clinical documents (PDFs) are stored in the App's private sandboxed storage, inaccessible to other applications.
- The speech-to-text model is stored locally and contains no personal or clinical data.

5.2 In Transit

All communication between the App and the Clinically API is encrypted using TLS 1.2 or higher.

5.3 Cloud Infrastructure

The Clinically API and all clinical data are hosted in Sydney, Australia. For full details on cloud infrastructure security, refer to the Clinically Platform Privacy Policy.

6. Data Retention on Device

- **On logout:** Authentication credentials, cached API responses, and temporary files (including downloaded PDFs) are cleared from the device.
- **Cache expiry:** Even while logged in, cached clinical data expires automatically within 2-10 minutes and is refreshed from the server.
- **Speech-to-text model:** The Whisper model file persists on-device until the App is uninstalled. It contains no personal data.
- **Uninstallation:** Removing the App deletes all App data from the device, including secure storage, cached data, and downloaded models.

7. Your Rights and Choices

7.1 Permission Controls

You can grant or revoke any device permission at any time through your device's Settings app. Revoking a permission will disable the associated feature but will not affect other App functionality.

7.2 Push Notification Content

Push notifications may include patient names to provide clinical context. If this is a concern in your environment, you can disable notifications in your device settings or configure notification previews to hide content when your device is locked.

7.3 Data Access and Deletion

As the App processes clinical data on behalf of your healthcare practice, requests for data access, correction, or deletion should be directed to your practice administrator. For queries about data Clinically holds as a processor, contact us using the details in Section 2.

7.4 Australian Privacy Act

Clinically complies with the Australian Privacy Principles (APPs) under the Privacy Act 1988 (Cth). If you believe your privacy has been breached, you may:

1. Contact us at hello@clinically.com.au
2. If unresolved, lodge a complaint with the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au or by calling 1300 363 992.

8. Children's Privacy

The App is not directed at children and is intended solely for use by healthcare professionals. We do not knowingly collect personal information from anyone under 18 years of age.

9. Changes to This Policy

We may update this policy to reflect changes in the App's functionality, legal requirements, or our practices. Material changes will be communicated through the App or via email. The effective date at the top of this document indicates when the policy was last revised.

10. Contact Us

If you have any questions about this privacy policy or how the App handles your data:

- **Email:** hello@clinically.com.au
- **Phone:** +61 2 4092 7710
- **Address:** Suite 2, 710 Hunter Street, Newcastle West NSW 2302, Australia

Change History

Version	Date	Author	Change Summary
1	22 Mar 2026	Wojt Janowski	# Change Summary: Clinically Mobile App — Privacy Policy **Document:** Clinically Mobile App — Privacy Policy **Previous Version:** No previous version exists **Current Version:** 1.0 (Effective 23/03/2026) --- ## Summary This is a **new document** — there is no previous version to compare against. Version 1.0 establishes the inaugural privacy policy for the Clinically mobile application. Key elements introduced include: - **Scope and audience:** Policy applies specifically to the Clinically mobile app for healthcare professionals (not patients), supplementing the broader Clinically Platform Privacy Policy (PRV-001). - **Data controller/processor distinction:** The healthcare practice is identified as the data controller; Clinically acts as processor of clinical data under service agreements. - **Data collection:** Defines account/authentication data, clinical data (processed on behalf of practices), and device permissions (camera, location, microphone, background microphone, biometrics, push notifications, storage, network state, vibration). - **On-device processing:** Documents an on-device speech-to-text engine (OpenAI Whisper) with no audio transmitted off-device. - **Third-party services:** Limits third-party integrations to Firebase Cloud Messaging (Google) for push notifications and Sentry (Functional Software, Inc.) for error monitoring/performance. Explicitly states no analytics, advertising, or other third-party SDKs are included. - **Security measures:** Specifies AES-256 encryption for cached data, platform-

Version	Date	Author	Change Summary
			native secure storage (iOS Keychain / Android Keystore), TLS 1.2+ for data in transit, and sandboxed document storage. - **Data retention on device:** Cached clinical data expires within 2–10 minutes; all app data cleared on logout and uninstallation. - **Australian regulatory compliance:** References the *Privacy Act 1988* (Cth) and Australian Privacy Principles (APPs), with complaint escalation pathway to the OAIC. - **Push notification transparency:** Discloses that notifications may contain patient names, with guidance on managing notification previews. - **Cloud hosting:** Confirms all clinical data hosted in Sydney, Australia.