

Capstone – Mobile Application Terms of Use & Privacy Notice

Australia (Privacy Act 1988 (Cth) & Australian Privacy Principles) | Apple App Store & Google Play aligned

Version: v1.0 | Date: 15 May 2026

Important notice

These Terms of Use & Privacy Notice (Terms) govern access to and use of the mobile application (the App) and any related services. The App is intended to be used in connection with the Supplier's Australian healthcare software platform (the Platform). If you do not agree to these Terms, you must not download, access or use the App.

1. Definitions

- **App** – the Capstone mobile application made available through the Apple App Store and/or Google Play.
- **Supplier** – Capstone Systems Pty Ltd (and its related bodies corporate) that provides the App and the Platform.
- **Customer** – the clinic, practice, organisation or business that holds a current subscription or licence to the Platform.
- **Authorised User** – a person authorised by the Customer to access the App and Platform (for example, staff, contractors, clinicians).
- **Customer Data** – information uploaded to, entered into, or generated within the App or Platform by or on behalf of the Customer, including patient records.
- **Personal Information** – has the meaning given in the Privacy Act 1988 (Cth).
- **Health Information** – is a category of sensitive information and includes information or an opinion about an individual's health or a health service provided to an individual, among other things.

2. Scope and acceptance

2.1 These Terms apply to all access to and use of the App by Customers and Authorised Users. Where the Customer has a separate master subscription agreement for the Platform, these Terms operate as a mobile application addendum.

2.2 By creating an account, signing in, or otherwise using the App, you confirm that you are an Authorised User and you agree to comply with these Terms and all applicable laws.

3. Licensed product – no sale

3.1 The App is licensed, not sold. Subject to these Terms and the Customer's current subscription/licence to the Platform, the Supplier grants a limited, revocable, non-exclusive, non-transferable, non-sublicensable licence to install and use the App on devices you own or control solely for the Customer's internal business purposes.

3.2 All rights not expressly granted are reserved by the Supplier. The Supplier retains all intellectual property rights in and to the App, the Platform, and all related materials.

3.3 App Store / Play Store usage rules apply. Your use of the App must also comply with the applicable platform terms, including Apple's and Google's usage rules and policies.

4. Accounts, authentication and access control

4.1 Access is limited to Authorised Users. The Customer is responsible for provisioning and de-provisioning access, applying role-based access controls, and ensuring access is removed immediately when a user is no longer authorised.

4.2 Credentials must not be shared. Each Authorised User must use their own login credentials and must keep those credentials confidential.

4.3 Device security. Authorised Users must maintain device-level security controls (for example, device PIN/biometrics, OS updates) and must not use the App on compromised devices (including jailbroken/rooted devices) where this could increase security risk.

5. Privacy, health data and Australian Privacy Principles

5.1 The Supplier is committed to protecting Personal Information and Health Information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs).

5.2 Roles. In most deployments, the Customer is the controller/owner of Customer Data (including patient records) and the Supplier acts as a service provider/processor to host and process that data to provide the App and Platform.

5.3 Collection and use. The App is designed to access and process Customer Data only as required to provide App functionality. The Supplier does not sell patient data and does not use Customer Data for unrelated advertising.

5.4 Consent and authority. The Customer is responsible for ensuring it has all necessary authorities, consents, and notices in place to collect and use Health Information and to allow Authorised Users to access it via the App.

5.5 Data minimisation. Authorised Users must only access, enter, or disclose patient information that is reasonably necessary for their role and for providing healthcare services or practice operations.

6. Privacy notice (App Store & Play Store friendly summary)

This section summarises the App's typical data handling in plain language.

6.1 Data we may collect or process

- Account and identity data (e.g., name, work email, role, clinic/practice identifier).
- Patient and clinical data entered by Authorised Users (e.g., notes, treatment records, appointments, invoices, images and documents) where the Customer uses these features.
- Device and technical data (e.g., device model, OS version, app version, diagnostic logs) to maintain security, troubleshoot and improve reliability.
- Usage and audit data (e.g., time of access, actions performed) to support security monitoring, compliance, and operational support.

6.2 How we use data

- Provide core App and Platform functionality (secure access to the Customer's account and records).
- Authenticate users, enforce permissions, and maintain audit trails.
- Prevent, detect and respond to security incidents and misuse.
- Provide support, maintenance and service communications.

6.3 Sharing and disclosures

We disclose Personal Information and Health Information only as necessary to provide the services, to the Customer (as the data owner/controller), to authorised service providers (for example, hosting and security providers), or where required by law.

6.4 Data location (Australia)

Unless otherwise agreed in writing, Customer Data is stored in computer data centres physically located within Australia.

6.5 Retention and deletion

Customer Data is retained in accordance with the Customer's instructions, contractual requirements, and applicable laws. On termination, data return and deletion processes follow the Customer's agreement for the Platform.

6.6 Your choices and access

Individuals may request access to or correction of their Personal Information. In a healthcare setting, these requests are typically handled through the Customer as the health service provider.

6.7 Privacy contact

Privacy enquiries and complaints: support@capstonesystem.com.au | [7 Phipps Cl, Canberra Australian Capital Territory 2600](#).

7. Security and confidentiality

7.1 The Supplier implements reasonable administrative, technical and physical safeguards designed to protect Customer Data against unauthorised access, loss, misuse or disclosure.

7.2 The Customer and Authorised Users must take reasonable steps to protect confidentiality, including preventing screenshots or screen recordings of patient records where not clinically necessary, and ensuring information is not copied into insecure channels (such as personal email, consumer messaging apps, or personal cloud storage).

7.3 No copying or bulk export. Authorised Users must not copy, scrape, harvest, bulk export, or reproduce patient records or other Customer Data from the App or Platform except where explicitly permitted by the Customer's policies and the Platform's authorised export tools.

7.4 Incident reporting. The Customer must notify the Supplier promptly of any suspected unauthorised access, credential compromise or security incident involving the App or Platform.

8. Prohibited conduct

You must not (and must not attempt to):

- access or use the App or Platform other than as an Authorised User for the Customer's internal business purposes;
- circumvent, disable or interfere with security features, authentication or access controls;
- reverse engineer, decompile, disassemble or attempt to derive source code (except to the extent permitted by law);
- use automation, bots or scraping to extract data;
- upload malware or attempt to interfere with the App's availability or performance;
- use the App in a way that breaches any law, clinical obligation, or the Customer's policies.

9. Mobile platform terms (Apple and Android)

9.1 The App may be accessed via Apple iOS devices and/or Android devices. Apple and Google are not responsible for the App, its content, or the services provided via the App.

9.2 Apple-specific acknowledgement. If you access the App on an iOS device: (a) Apple is not responsible for maintenance or support; (b) Apple has no obligation to provide any services in relation to the App; and (c) Apple and Apple's subsidiaries are third-party beneficiaries of these Terms and may enforce them against you.

9.3 Google/Android-specific acknowledgement. If you access the App via Google Play: (a) Google is not responsible for maintenance or support; and (b) you must comply with Google Play policies and terms.

10. Support and updates

10.1 The Supplier may provide updates, patches and enhancements from time to time. Some updates may be mandatory for security reasons.

10.2 Support is provided by the Supplier (not Apple or Google) via: [SUPPORT EMAIL] and/or [SUPPORT PORTAL URL].

11. Clinical and professional use disclaimer

11.1 The App is a tool to support workflow and access to information. It does not provide medical advice and is not a substitute for professional clinical judgement.

11.2 The Customer remains responsible for clinical decisions, regulatory compliance, record keeping obligations, and ensuring appropriate procedures exist outside the App to manage risks in its practice.

12. Suspension and termination

12.1 The Supplier may suspend or terminate access to the App (in whole or part) where reasonably necessary to: protect security; prevent misuse; comply with law; or address a material breach of these Terms.

12.2 On termination or expiry of the Customer's Platform subscription/licence, the right to use the App ends.

13. Liability

13.1 To the maximum extent permitted by law, the Supplier excludes liability for indirect or consequential loss and for loss arising from misuse of the App, compromised devices, or the Customer's failure to maintain appropriate policies and controls.

13.2 Nothing in these Terms excludes any consumer guarantees that cannot be excluded under the Australian Consumer Law; however, where permitted, remedies may be limited.

14. Governing law

These Terms are governed by the laws specified in the Customer's master subscription agreement for the Platform. If no governing law is specified, the laws of the Australian Capital Territory apply.

Annex A – Policies

- Data Security Policy: [URL]
- Privacy Policy: [URL]

By downloading, installing, or using the App, you acknowledge that you have read and understood these Terms and agree to be bound by them.

Privacy Policy – Capstone Systems Pty Ltd

Effective Date: 15 May 2026

1. Overview

Capstone Systems Pty Ltd (we, us, our) is committed to protecting personal and health information in accordance with the Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs). This Privacy Policy describes how we handle personal information in connection with our mobile application and backend healthcare system (Capstone Platform).

2. Scope

This policy applies to authorised staff users of healthcare providers who access the Capstone Platform via the mobile application. We act primarily as a service provider (data processor) on behalf of our customers (healthcare organisations).

3. Information We Handle

- Personal Information: name, email, role details
- Health Information: patient records, treatment data
- Technical Data: device type, logs, usage activity
- Audit Logs: access, edits, and system interactions

4. Purpose of Use

- Provide secure access to healthcare systems
- Maintain audit trails for compliance
- Support clinical workflows
- Detect and prevent security incidents

5. Data Storage and Security

Data is stored in Microsoft Azure data centres located in Australia. No patient data is stored locally on mobile devices. Strong encryption, role-based access control, and mandatory multi-factor authentication are enforced.

6. Data Sharing

We do not sell personal information. Data may be disclosed to cloud hosting providers (Microsoft Azure) and communication providers where necessary to deliver services.

7. Data Protection Measures

- Encryption in transit and at rest
- Mandatory MFA
- Comprehensive audit logging
- Access controls
- Regular monitoring and security reviews

8. Data Breaches

We comply with the Notifiable Data Breaches scheme and will notify affected entities where required by law.

9. Contact

Capstone Systems Pty Ltd
Canberra, ACT

support@capstonesystem.com.au

Data Security & Data Loss Prevention Policy – Capstone Systems Pty Ltd – Mobile App

Effective Date: 15 May 2026

1. Purpose

This policy outlines controls implemented to protect sensitive healthcare data and prevent data loss.

2. Data Classification

- Sensitive: Health Information
- Personal: Staff identifiers
- Operational: Logs, system data

3. Access Control

Access is role-based and requires mandatory multi-factor authentication. Credential sharing is prohibited.

4. Data Storage

All data is stored securely in Microsoft Azure within Australia. No persistent data is stored on user devices.

5. Data Loss Prevention Controls

- No local storage of patient data
- Restrictions on copying/exporting data
- Monitoring of unusual activity
- Prevention of unauthorised exports
- Secure communications controls

6. Monitoring and Logging

All user activity is logged, including access, modification, and system actions, to support auditing and investigations.

7. Incident Response

Security incidents are investigated and managed promptly. Notifications are issued in accordance with Australian law.

8. Responsibilities

Users must follow security policies, protect credentials, and report incidents immediately.

9. Enforcement

Non-compliance may result in access suspension or termination.

10. Contact

support@capstonesystem.com.au