



EFFICCA

Security and privacy, built for sensitive care data.

Efficca protects sensitive care and operational information using managed Google Cloud and Supabase services in Sydney, layered access controls, encryption, privacy-aware AI and tested recovery safeguards.

Version 1.8 | Reviewed 20 October 2026

EIGHT PRACTICAL SAFEGUARDS

01 Managed Sydney cloud foundation Customer data is not hosted on office servers. Supabase provides the primary database, authentication, file storage and realtime services in Sydney. Google Cloud runs the web application, background processing, document OCR, secrets, recovery and Efficca's own document search model in Sydney. Melbourne holds a live standby copy, about 30 seconds behind, and hourly backup copies.	02 Controlled access Tenant separation, row-level security, role, branch and folder permissions, and audit trails restrict access to authorised users and activities. Two-step sign-in, with an authenticator app or a passkey, is required for staff on the web and the phone app from 20 October 2026.
03 Encryption and key management Data is encrypted in transit and through infrastructure encryption at rest. Independent backup copies in Sydney and Melbourne each use a customer-managed key through Google Cloud KMS. Selected high-risk records receive additional application-level encryption.	04 Privacy-aware AI AI follows user permissions and privacy settings. People review outputs and approve record changes. See our Privacy Policy for providers, data handling and retention.
05 Security governance and response Code and configuration changes pass automated security checks, secret scanning, dependency monitoring and controlled release gates. Security findings are triaged according to risk. Documented incident procedures cover reporting, containment, assessment, recovery and customer or regulator notification where required.	06 Resilience and recovery Point-in-time recovery covers 14 days, and a live standby database copy in Melbourne runs about 30 seconds behind. Backups are CMEK-encrypted, copied every hour from Sydney to Melbourne and kept 35 days in each region, files included. Efficca has completed isolated recovery exercises from both regions.
07 Restricted Efficca personnel access Customer information may be accessed only by authorised Efficca personnel who need it for their role in operating, supporting or securing the service. Administrative access is permission-scoped, and each Efficca support visit to a customer account is recorded with the reason given.	08 A record of who did what Efficca keeps an activity record for your organisation: who did what, and when, naming the person or automatic process behind each entry. Personal and health details are hidden inside the change details. Efficca's app and background services can only add entries, the only change allowed is hiding a value for privacy (and that change is recorded too), and entries are kept for 7 years. Owners, and auditors they invite, can search it, see what changed and export any period.

Independent certification

AI Core CRM Pty Ltd, the company behind Efficca, is certified to ISO/IEC 27001:2022 for the Efficca platform (certificate SIS010725I048, SIS Certifications; next surveillance audit June 2027). Google Cloud, Supabase and AWS publish their own ISO/IEC 27001 and SOC 2 assurance, which apply to the suppliers' own service boundaries. Supabase publishes ISO/IEC 27001 and SOC 2 Type 2 assurance; Supabase's Sydney region runs on AWS infrastructure.

Verify certificate SIS010725I048 | Google Cloud ISO/IEC 27001 | Google Cloud SOC 2 | Google Cloud encryption and Cloud KMS | Supabase security | Supabase SOC 2 Type 2 | Supabase regions | AWS compliance programmes | AWS ISO/IEC 27001 | AWS SOC reports

WHERE DATA SITS, MOVES AND EXPIRES

SYDNEY CORE Core operational records are hosted in Australia. Supabase services, Google Cloud application, background and OCR services, and workflow orchestration are configured in Sydney; document search runs on Efficca's own search model in Sydney. A live standby copy and backup copies are also kept in Melbourne.	DISCLOSED SUPPORTING SERVICES See our Privacy Policy for service providers, processing locations and safeguards.	LIFECYCLE AND REQUESTS Efficca supports requests for access, correction, export and deletion where available. Information is retained while needed to provide and secure the service, follow provider instructions and meet applicable legal, financial, safeguarding, audit and NDIS record-keeping obligations. Recovery copies expire through their backup schedules.
--	--	--

Security works best as a shared practice

These controls support providers in meeting obligations under the Australian Privacy Principles and NDIS information-security requirements. Providers remain responsible for lawful collection, access administration and regulated decisions.

Need evidence for procurement or due diligence?

Ask us for the current sub-processor list, supplier trust material or help with a security questionnaire. Architecture and confidential evidence can be provided through an appropriate review process.

Download PDF | View Privacy | View Sub-processors | Request a security review