EFFICA

Security and privacy, built for sensitive care data.

Effica 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 1.2 | Reviewed 19 August 2026

SEVEN 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 from its Sydney region. Google Cloud provides the web application, regional load balancing, background processing, private media processing, secrets and recovery services in Sydney.

02 Controlled access

Tenant separation, row-level security, role, branch and folder permissions, and audit trails restrict access to authorised users and activities. Secure authentication and protected sessions are used, and MFA is supported for user accounts.

03 Encryption and key management

Data is encrypted in transit and through infrastructure encryption at rest. Independent Sydney backup copies use a customer-managed key through Google Cloud KMS. Selected high-risk records receive additional application-level encryption.

04 Privacy-aware AI

AI access follows the user's permissions and the task's purpose. Help that uses a named participant's record stays off until a recorded yes, and processing stops while the switch is off. Raw documents, images and audio are processed through private Sydney services before any later text step. Customer data is not opted into provider model training. We are working toward OpenAI Zero Data Retention, and important decisions require human review.

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

Production database point-in-time recovery is configured for 14 days. Independent Sydney backups are CMEK-encrypted and retained for 35 days, durable files are covered, and Effica has completed a successful isolated recovery exercise.

07 Restricted Effica personnel access

Customer information may be accessed only by authorised Effica personnel who need it for their role in operating, supporting or securing the service. Administrative access is permission-scoped and sensitive actions are logged.

Independent supplier assurance

Google Cloud publishes ISO/IEC 27001 and SOC 2 assurance, Supabase publishes ISO/IEC 27001 and SOC 2 Type 2 assurance, and AWS publishes ISO/IEC 27001 and SOC reports. These assurances apply to the suppliers' own service boundaries; they do not certify Effica or its customers. Supabase's Sydney region runs on AWS infrastructure, while Effica's application runtime and background services run on Google Cloud in Sydney.

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 database, authentication and file storage, and Google Cloud application, background, document and image, and raw-audio services are configured in Sydney.

DISCLOSED SUPPORTING SERVICES

Some disclosed supporting services may process limited information overseas for specific purposes, including protected AI text and email delivery. Effica discloses these services and applies data minimisation, access controls, contractual protections and security safeguards appropriate to each service.

LIFECYCLE AND REQUESTS

Effica 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