Clinically

Security Overview for Customers

Standard

Code: GOV-004

Version: 1

Effective Date: 25 Mar 2026

Review Date: 25 Mar 2027

Author: Wojt Janowski

Approved By: Wojt Janowski (25 Mar 2026)

Owner: Wojt Janowski

1. Introduction

Clinically is a cloud-based clinical workflow management platform built for Australian healthcare providers. We help specialist clinics, radiology practices, and allied health practices manage referral triage, patient records, clinical documents, practice communications, and appointment scheduling.

We understand that healthcare organisations considering our platform need confidence that patient health information will be protected to the highest standard. This document provides an overview of our security architecture, data protection controls, and compliance posture to support your evaluation.

This document is intended for practice managers, IT decision-makers, and procurement teams evaluating the Clinically platform. For detailed privacy information, please refer to our Privacy Policy. For specific security questions not covered here, please contact us at security@clinically.com.au.

2. Platform Overview

Clinically is a multi-tenant Software-as-a-Service (SaaS) platform hosted entirely within Australian data centres. The platform is built on modern, well-supported frameworks and infrastructure:

- **Database:** PostgreSQL with database-per-tenant isolation
- **File storage:** AWS S3 with custom envelope encryption
- **Infrastructure:** Amazon Web Services (AWS), Sydney region (ap-southeast-2)
- **Edge security:** Cloudflare for DDoS protection, CDN, and TLS termination

3. Australian Data Residency

All patient data is stored and processed within Australia. This includes:

- **Databases:** AWS, Sydney region
- **File storage:** AWS S3, Sydney region
- **Backups:** AWS S3, Sydney region
- **Email processing:** AWS SES (Sydney) and SMTP2GO (Australian data centres)
- **AI document processing:** AWS Bedrock, Sydney region
- **SMS and fax delivery:** Australian provider (Notifyre)

Payment processing (Stripe) is the only service where non-patient data leaves Australia — only organisation billing information is sent to Stripe. No patient health information, government identifiers, or clinical data is transferred overseas.

Cloudflare provides DDoS protection and content delivery. HTTP requests transit through global edge servers but data is processed in memory only and is not persistently stored outside Australia.

We maintain a detailed sub-processor register documenting all third-party services, their data handling practices, and jurisdictional information. This register is available to customers on request.

4. Tenant Isolation

Clinically uses a **database-per-tenant** isolation model. Each healthcare practice on our platform receives:

- A **dedicated PostgreSQL database** — your patient data is physically separated from every other practice on the platform
- **Unique encryption keys** — each practice has its own master encryption key for file encryption, independent of all other practices
- **Isolated session storage** — user sessions are stored within your practice's database, not in a shared session store
- **Separate storage paths** — files and documents are stored in practice-specific paths within encrypted storage

This means that a security incident affecting one practice's data cannot expose another practice's patients. Even in the unlikely event of a session hijack or fixation attack, the physical separation of session stores prevents cross-practice leakage.

This level of isolation exceeds the industry norm for multi-tenant SaaS platforms, which typically use a single shared database with logical row-level separation.

5. Encryption

5.1 Files at Rest

All clinical documents, attachments, and uploaded files are protected by a multi-layered envelope encryption system:

- **Every file** is encrypted with its own unique data key
- **Each data key** is wrapped (encrypted) with the practice's master key

- **The encryption algorithm** is XChaCha20-Poly1305 — an authenticated encryption cipher that both encrypts the data and detects any tampering or corruption
- **Key material** is explicitly cleared from memory after each operation
- **Streaming encryption** handles large files efficiently without loading the entire file into memory

This means that even if raw file storage were accessed, the files cannot be read without the corresponding encryption keys. And because each practice has its own master key, a compromised key affects only that single practice.

5.2 Database Fields

Sensitive database fields are individually encrypted at the application level, including:

- Medicare numbers
- DVA numbers
- Individual Healthcare Identifiers (IHIs)
- Dates of birth

A database export without the application encryption keys does not expose these fields in plaintext.

5.3 Data in Transit

- **Browser to server:** All traffic is encrypted via HTTPS. HTTP Strict Transport Security (HSTS) is enforced with a one-year duration including subdomains.
- **Application to database:** PostgreSQL connections use SSL encryption.

5.4 Backups

Database backups are encrypted at rest using AES-256 server-side encryption. Backups follow a managed lifecycle: 30 days in standard storage, then 150 days in archival storage, then automatic deletion at 180 days.

6. Authentication and Access Control

6.1 Authentication Options

Clinically supports multiple authentication methods, configurable per practice:

- **Password with two-factor authentication (2FA):** Passwords are hashed with bcrypt (12 rounds). TOTP-based two-factor authentication adds a second layer of protection.

- **Single sign-on (SSO):** SSO with per-practice identity provider configuration, allowing integration with your existing identity management.
- **Passkeys (WebAuthn):** Phishing-resistant passwordless authentication using device-based cryptographic credentials.

Practices can enforce security policies such as mandatory 2FA or mandatory SSO for all users, with grace periods for policy transitions.

6.2 Brute-Force Protection

- Login attempts are rate-limited per IP address with automatic lockout after failed attempts
- Anti-enumeration protections prevent attackers from determining whether an account exists based on response timing or content

6.3 Role-Based Access Control

Within each practice, access is controlled through a permission-based system:

- **Route-level permissions** gate access to features by user role (e.g., only users with the "view referrals" permission can access the referrals module)
- **Model-level policies** enforce access control on individual records

6.4 Session Security

- **Session fingerprinting** detects session hijacking by monitoring for changes in IP address, browser, and other characteristics
- **Concurrent session detection** identifies unusual login patterns
- **Automatic invalidation** of all sessions on password change, 2FA toggle, or security policy change
- **Encrypted session storage** within the practice's isolated database

7. AI-Assisted Document Processing

Clinically uses artificial intelligence to help practices process incoming clinical documents more efficiently:

- **Document classification:** AI determines whether an incoming document is a referral, pathology result, radiology report, or other document type
- **Patient data extraction:** AI extracts patient details from documents to assist with record matching

- **Conversation summaries:** AI generates brief summaries of resolved communication threads

Key safeguards:

- AI processing uses **AWS Bedrock in the Sydney region** — patient data does not leave Australia for AI processing
- The AI provider **does not use patient data to train models** and does not retain data after processing
- AI outputs are presented for **human review** — AI assists staff, it does not make clinical decisions
- AI processing is **logged** in the practice's database for auditability
- We are actively working to **minimise patient-identifiable information** in AI processing where identification is not required

8. Infrastructure Security

8.1 DDoS and Edge Protection

Cloudflare provides layered protection at the network edge, including DDoS mitigation, web application firewall capabilities, and bot management. Cloudflare Turnstile CAPTCHA is available on public-facing forms to prevent automated abuse.

8.2 Security Headers

The platform enforces security headers on all responses, including HSTS, clickjacking protection (X-Frame-Options), MIME type sniffing protection, referrer policy controls, and permissions policy restricting access to device features.

8.3 Input Validation and Malware Protection

- **Virus scanning:** All incoming documents and email attachments are scanned using ClamAV antivirus and AWS SES virus verdict checking
- **File size limits:** Pre-checks prevent oversized uploads from consuming resources
- **Input validation:** All user input is validated at the application boundary using framework-level validation rules
- **Rate limiting:** All public-facing endpoints are rate-limited to prevent abuse

8.4 Webhook and Integration Security

Inbound webhooks from third-party services (email notifications, SMS/fax delivery confirmations) are protected by cryptographic signature validation, per-IP rate limiting, and message deduplication.

9. Monitoring and Audit

- **Security event logging:** Authentication attempts, permission changes, data access, session events, and policy enforcement are logged with structured context (IP address, user agent, timestamp, user, and practice)
- **365-day audit log retention** within each practice's isolated database
- **Application performance monitoring** for service health and availability
- **Queue monitoring** for background job processing visibility
- **Health checks** with automated alerting for service degradation

10. Backup and Recovery

- **Automated daily backups** of all practice databases to encrypted storage
- **Managed backup lifecycle:** 30 days standard access, 150 days archival, 180 days total retention
- **Backup restoration testing** conducted regularly to verify recoverability
- **Recovery objectives** are tiered by service criticality, with patient-impacting services receiving the highest priority

11. Personnel Security

- All personnel undergo **pre-engagement screening** proportionate to their access level
- **Confidentiality and non-disclosure agreements** are required before any system access is granted, with obligations surviving the end of engagement
- **Security onboarding** covers the nature of health data processed, key policies, and reporting obligations
- **Separation procedures** include immediate access revocation, credential rotation, and audit log review
- **Code review** is mandatory for all changes — no code reaches production without peer review

12. Software Development Security

- **Static analysis** runs on every code change and must pass before deployment
- **Automated test suite** covering authentication, authorisation, encryption, and tenant isolation
- **Dependency scanning:** Daily automated scanning for known vulnerabilities in third-party libraries
- **Secret scanning:** Pre-commit hooks prevent accidental credential commits
- **Branch protection:** The main codebase requires pull request review, passing static analysis, and passing tests before any change is accepted
- **Environment separation:** Production, staging, and development environments are strictly separated. Patient data is never used in non-production environments.

13. Compliance Framework

Clinically's security and privacy programme is aligned with the following Australian and international frameworks:

13.1 Australian Regulatory

- **Privacy Act 1988 (Cth)** and the **Australian Privacy Principles (APPs)** — our platform is designed to support healthcare practices in meeting their APP obligations
- **Notifiable Data Breaches (NDB) scheme** — we maintain a documented Data Breach Response Plan compliant with Part IIIC of the Privacy Act
- **My Health Records Act 2012** and **Healthcare Identifiers Act 2010** — relevant controls are implemented for the handling of Medicare numbers, IHIs, and healthcare identifiers

13.2 Security Standards

- **ASD Essential Eight** — informs our security baseline as the Australian Government's recommended mitigation strategies
- **SOC 2** — our policy framework provides coverage across all SOC 2 Trust Services Criteria (Security, Availability, Processing Integrity, Confidentiality, Privacy). Formal SOC 2 certification is on our roadmap.
- **ISO/IEC 27001:2022** — our Information Security Management System (ISMS) is structured to align with ISO 27001 Annex A controls. Formal certification is a longer-term objective.

13.3 Governance Documentation

We maintain a comprehensive suite of governance and security documentation including:

- Information Security Management Policy (ISMS)
- Risk Management Framework with active risk register
- Privacy Impact Assessment
- Data Breach Response Plan
- Business Continuity and Disaster Recovery Plan
- Access Control and Identity Management Policy
- Data Processing Integrity Policy
- Personnel Security Policy
- Asset Management and Classification Policy
- Secure Development and Technical Operations Policy
- Sub-Processor Register
- Privacy Policy

These documents are reviewed on a regular cycle and updated after significant platform changes or security incidents.

14. Shared Responsibility

Security is a shared responsibility between Clinically and the healthcare practices that use our platform:

Clinically is responsible for	Your practice is responsible for
Platform infrastructure security	Managing user accounts and permissions within your practice
Encryption of data at rest and in transit	Enforcing appropriate security policies (2FA, SSO) for your users
Tenant isolation and access controls	Training staff on appropriate use of the platform
Security monitoring and incident response	Reporting suspected security incidents to us promptly

Backup and disaster recovery	Maintaining your own privacy policy and patient consent processes
Vulnerability management and patching	Reviewing and responding to data access requests from patients
Compliance with our security policies	Configuring integrations (EMR sync, webhooks) appropriately

15. Contact

For security questions, due diligence requests, or to report a vulnerability:

Email: security@clinically.com.au

For privacy enquiries:

Email: privacy@clinically.com.au

We are happy to provide additional documentation, answer specific security questionnaires, or arrange a security briefing as part of your evaluation process.

Change History

Version	Date	Author	Change Summary
1	25 Mar 2026	Wojt Janowski	Minor adjustments