Clinically

Sub-Processor Register

Record

Code: PRV-002

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

This policy complies with: Australian Privacy Principles; SOC 2; ISO 27001; Healthcare Identifiers Act 2010; ADHA Conformance

About This Document

This register lists all third-party sub-processors that process personal information on behalf of healthcare practices using the Clinically platform. It is maintained to support compliance with APP 8 (cross-border disclosure) of the Australian Privacy Principles and to provide transparency to customers during procurement and due diligence.

Definitions

- **Sub-processor:** A third party that processes personal information on behalf of Clinically in connection with providing the platform to healthcare practices.
- **Tenant-directed:** Data exchange initiated and configured by the healthcare practice. Clinically facilitates the integration but the practice controls what data is shared.
- **DPA:** Data Processing Agreement — a contractual agreement that governs how the sub-processor handles personal information, including security obligations, data residency, and breach notification.
- **Cross-border:** Whether personal information is transferred to, or processed in, a jurisdiction outside Australia.

Summary

Sub-Processor	Service	Data Types	Location	Cross-Border	DPA
AWS	Infrastructure, AI	All patient data	Australia	No	**On file**
Cloudflare	DDoS, CDN, TLS	HTTP data (transient)	Global	Yes (transient)	**On file**
SMTP2GO	Email relay	Email content	Australia	No	**On file**
Notifyre	SMS, Fax	Phone numbers, message content	Australia	Verify	**On file**

Stripe	Billing	Organisation billing data	US	Yes (no patient data)	**N/A**
Slack	Error alerts	Error logs (no patient data)	US	Yes (no patient data)	**N/A**
Halaxy	EMR sync	Patient data (tenant-directed)	Australia	No	**N/A**
Genie	EMR sync	Patient data (tenant-directed)	Australia (local)	No	**N/A**
Services Australia	Medicare/IHI	Gov identifiers, demographics	Australia	No	**N/A**

Self-hosted services (not sub-processors): Meilisearch (search indexing), ClamAV (virus scanning), ocrmypdf (document OCR). These run within our own infrastructure and do not send data to third parties.

Detailed Sub-Processor Profiles

1. Amazon Web Services (AWS)

Legal entity	Amazon Web Services, Inc.
Services used	S3 (file storage), RDS (PostgreSQL databases), SES (email send/receive), SNS (webhook notifications), Bedrock (AI document classification and patient data extraction)
Jurisdiction	Australia (ap-southeast-2, Sydney)
Cross-border transfer	No. All services configured in ap-southeast-2. Bedrock processing remains in-region. AWS does not replicate data outside the configured region.
Security certifications	SOC 1/2/3, ISO 27001, ISO 27017, ISO 27018, IRAP (Australian Government), PCI DSS, HIPAA eligible
AI data handling	Bedrock: prompts and responses are not used to train models. No data retention after processing. AWS commits to not accessing customer data

	except as necessary to provide the service.
DPA in place	Yes
Last reviewed	23 March 2026

Data processed:

- All patient data: demographics, clinical documents, health information, communications, appointments, form submissions
- Government identifiers (Medicare, DVA, IHI) — encrypted at field level
- Clinical documents — envelope encrypted with per-tenant keys
- AI processing: document text including patient names, health conditions, Medicare numbers (Bedrock)
- Database backups (encrypted at rest)

2. Cloudflare, Inc.

Legal entity	Cloudflare, Inc.
Services used	DDoS protection, CDN (content delivery network), TLS termination, DNS, Turnstile CAPTCHA on public forms
Jurisdiction	Global edge network
Cross-border transfer	Yes — HTTP requests transit through the nearest Cloudflare edge node, which may be outside Australia. Data is processed in memory only and not persistently stored. Cloudflare's Data Localisation Suite is available if required.
Security certifications	SOC 2 Type II, ISO 27001, PCI DSS Level 1, HIPAA compliant
DPA in place	Yes
Last reviewed	23 March 2026

Data processed:

- HTTP request/response data (transient — in memory during request processing)
- IP addresses, HTTP headers, request URLs
- No persistent storage of patient data

3. SMTP2GO

Legal entity	SMTP2GO (a Mailguard company)
Services used	Outbound email relay for practice inbox communications
Jurisdiction	Australia (Australian data centres configured for this account)
Cross-border transfer	No. Account configured to use Australian data centres.
Security certifications	SOC 2, SPF/DKIM/DMARC support, TLS encryption in transit
DPA in place	Yes
Last reviewed	04 March 2026

Data processed:

- Email addresses (sender and recipient)
- Email content — may contain patient names, health information, appointment details, clinical correspondence
- Email delivery status and metadata

4. Notifyre

Legal entity	Notifyre Pty Ltd
Services used	SMS delivery to patients and referrers; fax delivery and receipt
Jurisdiction	Australia (verify)
Cross-border transfer	Verify with Notifyre whether any data is processed or stored outside Australia.

Security certifications	HMAC webhook signature validation, TLS in transit
DPA in place	Yes
Last reviewed	23 March 2026

Data processed:

- Patient phone numbers
- SMS message content — may contain appointment details, practice communications
- Fax content — may contain clinical documents, referrals, pathology results
- Delivery status callbacks

5. Stripe

Legal entity	Stripe, Inc.
Services used	Subscription billing, payment processing for healthcare practice accounts
Jurisdiction	United States
Cross-border transfer	Yes — billing data only. No patient health information, government identifiers, or clinical data is transferred. Stripe is certified under the Data Privacy Framework.
Security certifications	PCI DSS Level 1, SOC 1/2, ISO 27001
DPA in place	Yes
Last reviewed	23 March 2026

Data processed:

- Organisation name, ABN, administrator email
- Stripe customer ID, subscription ID, payment method tokens

- No patient data is sent to Stripe

6. Slack Technologies (Salesforce)

Legal entity	Slack Technologies, LLC (Salesforce, Inc.)
Services used	Developer error notifications, system health alerts
Jurisdiction	United States
Cross-border transfer	Yes — operational/error data only. Error logging is configured to exclude patient-identifiable information. Stack traces may incidentally include request context but not patient records.
Security certifications	SOC 2/3, ISO 27001, ISO 27017, ISO 27018
DPA in place	N/A
Last reviewed	23 March 2026

Data processed:

- Application error messages, stack traces (truncated)
- System health check results
- No patient data in normal operation — errors are sanitised before dispatch

7. Halaxy

Legal entity	Halaxy Pty Ltd
Services used	EMR synchronisation — patient demographics, appointments, clinical documents exchanged at the tenant's direction
Jurisdiction	Australia
Cross-border transfer	No.

Security certifications	Australian healthcare EMR provider. Verify certifications directly with Halaxy.
DPA in place	N/A
Last reviewed	23 March 2026

Data processed:

- Patient demographics (name, DOB, gender, contact details)
- Appointments and scheduling data
- Clinical documents and referrals (where sync is configured)
- Data exchange is bidirectional and initiated by the tenant

8. Genie Solutions

Legal entity	Genie Solutions Pty Ltd (Citadel Health)
Services used	EMR synchronisation via bridge client — patient demographics, referrals, clinical documents
Jurisdiction	Australia (local installation at practice site)
Cross-border transfer	No. Genie is locally installed at the practice. Data exchange occurs between the Clinically platform and the local Genie instance.
Security certifications	Locally hosted. Security is managed by the practice's IT environment.
DPA in place	N/A
Last reviewed	23 March 2026

Data processed:

- Patient demographics, referrals, clinical documents
- Data exchanged via locally installed bridge client at the practice's direction

9. Services Australia (PRODA)

Legal entity	Services Australia (Australian Government)
Services used	Medicare and IHI verification via PRODA B2B authentication; provider number validation
Jurisdiction	Australia (Australian Government)
Cross-border transfer	No.
Security certifications	Australian Government security standards. PRODA B2B authentication with digital certificates.
DPA in place	N/A
Last reviewed	23 March 2026

Data processed:

- Medicare numbers, Individual Healthcare Identifiers (IHIs)
- Patient name and date of birth (for verification matching)
- Provider numbers

Change History

Version	Date	Author	Change Summary
1	25 Mar 2026	Wojt Janowski	# Change Summary: Sub-Processor Register This is a **new document** — no previous version exists for comparison. The document establishes the following: - **Created a Sub-Processor Register** to support transparency and compliance with APP 8 (cross-border disclosure) under the *Privacy Act 1988* (Cth) - **Defined key terms** including sub-processor, tenant-directed data exchange, DPA, and cross-border transfer - **Listed nine sub-processors** with summary details on service type, data processed, jurisdiction, cross-border status, and DPA status: - **AWS** — infrastructure and AI (Bedrock), all patient data, Australia (ap-southeast-2), DPA on file - **Cloudflare** — DDoS/CDN/TLS, transient HTTP data, global (cross-border), DPA on file - **SMTP2GO** — email relay, Australia, DPA on file - **Notifyre** — SMS and fax, Australia (cross-border status flagged for verification), DPA on file - **Stripe** — billing only (no patient data), US (cross-border), DPA marked N/A - **Slack** — error alerts only (no patient data), US (cross-border), DPA marked N/A - **Halaxy** — EMR sync (tenant-directed), Australia, DPA marked N/A - **Genie Solutions** — EMR sync via local bridge client (tenant-directed), Australia, DPA marked N/A - **Services Australia** — Medicare/IHI verification via PRODA, Australia, DPA marked N/A - **Provided detailed profiles** for each sub-processor covering legal entity, services used, jurisdiction, cross-border transfer rationale, security certifications, DPA status, last review date, and specific data

Version	Date	Author	Change Summary
			types processed - **Noted self-hosted services** (Meilisearch, ClamAV, ocrmypdf) that are explicitly excluded as sub-processors since they run within Clinically's own infrastructure - **Identified an open action item** for Notifyre regarding verification of cross-border data processing status