Kookaburra Health
Business intelligence for Australian allied health clinics

PLAIN-ENGLISH SUMMARY

Privacy & security at Kookaburra Health

For clinic owners considering or using Kookaburra Health. **Effective 2 June 2026 · Version 2.0.**

This is the plain-English version of how we handle your clinic's data. Our full Privacy Policy is the legally binding document; this page exists so you can understand it in five minutes.

Who we are and what we hold

Kookaburra Health is operated by **Principal Podiatry Pty Ltd** (ABN 19 615 606 347), an Australian company run by an AHPRA-registered podiatrist. We're an Australian Privacy Principles (APP) entity under the Privacy Act 1988 (Cth), and we treat your patient data as **sensitive health information** — the highest-protection category under Australian privacy law.

We connect to your practice-management system (Cliniko today; others coming) and compute clinic-level reports + a data chat. We do **not** receive patients directly. We do **not** provide clinical decisions. We are an operations and reporting tool for the practice owner.

Where your data lives — Australia only

Everything that touches your clinic's data stays in Australia:

- **Our servers** are hosted in Sydney by DigitalOcean.
- **Our database** is a managed Sydney cloud database with full disk encryption, TLS-only connections, and encrypted automated daily backups.
- **Chat conversations, API credentials, and patient identifiers** are additionally encrypted at the application layer with a key held by us. Even with full database access — ours or our hosting provider's — nobody can read your conversations or your patient identifiers without that application key. The plaintext exists only transiently in memory while a request is being processed.
- **Our AI processing** runs on Amazon Bedrock in **Sydney (ap-southeast-2) only**. Our access policy denies any AI invocation outside Australia — the system is technically incapable of calling AI in the US, Asia, or anywhere else, even if someone misconfigured it.
- **Cliniko** (the practice-management system we connect to) is also Australian-hosted.

That means your patient information never crosses the Australian border for any processing under our control. This is the strongest position we can take under APP 8 (cross-border disclosure), and it's the default architecture.

What the AI actually sees

Two important guarantees about the AI integration:

- **Aggregates, not patients.** By default, the AI receives only your clinic-level numbers (utilisation, recall rate, revenue mix, no-show rate, etc.) — never individual patient records, names, dates of birth, Medicare numbers, or clinical notes.
- **Opaque IDs for patient-level features.** When the AI references a patient (e.g. ranking the most-attended patients, surfacing a lapsed list), it sees a one-way cryptographic ID — think of it as a random code — never the patient's name. To turn a code into a real name you click an explicit "reveal" button, which creates an audit log entry showing who looked up whom and when.

The AI is **never given access to free-text clinical notes, diagnoses, Individual Healthcare Identifiers (IHIs), or My Health Record (MHR) data.** Those are out of scope by design.

Your data is never used to train AI

Under our AWS Bedrock agreement, **none of your data is used to train AI models** — not Anthropic's, not AWS's, not anyone's. Anthropic personnel have no access to the inference infrastructure on Bedrock. Your prompts and responses are processed and discarded. We hold the contractual evidence of this (the AWS Data Processing Addendum) and can provide it on request.

One clinic's data never sees another clinic's data

This is technical, but worth understanding:

- Every database query in our system is scoped to your account — we have verified this in our code review.
- The cryptographic ID we generate for your patients uses a **secret unique to your account**. Even if two clinics happened to have the same patient, the ID our system would generate is completely different for each. There is no way to "merge" or "cross-reference" patients between clinics.
- The AI processes one question for one clinic at a time. Nothing about your data persists in the AI between requests.

If you ever wanted to verify this independently, we will walk a privacy auditor through the relevant code.

Our full at-rest and in-transit posture

Layer	How it's protected
Server hosting	DigitalOcean Sydney
Application database	Managed cloud database (Sydney) — full disk encryption, TLS-only, encrypted automated backups
Chat conversations at rest	Authenticated symmetric encryption with a customer-managed key
API credentials at rest	Same encryption, same key
Patient identifiers at rest	Authenticated encryption on the source ID + one-way hashed opaque IDs scoped per clinic
AI inference	Claude on AWS Bedrock in Sydney (ap-southeast-2) only
Browser ↔ application	Modern TLS with HSTS + Secure cookies
Application ↔ database	TLS-only
Email	Major transactional email provider over HTTPS
Per-tenant isolation	Verified at database query + cryptographic-ID layers

What we log — and what we don't

We log technical metadata: when a request happened, how many tokens it used, the model version, error codes. We **do not** log the content of your prompts or the AI's responses to general application logs. Conversations in the chat are stored in our Sydney database (so you can see your history) but never exposed to third-party log services like error trackers.

You're in control

- **You can disconnect Cliniko any time** from your account settings; we stop pulling new data immediately.
- **You can delete your account**; we permanently delete your data within 30 days (legal retention requirements may apply to invoicing records).
- **Patient-level features can be turned off** on request; we immediately delete the de-identified patient warehouse and the lookup vault.
- **You can request the audit log** of any patient-reveal actions taken in your account.

Notifiable Data Breaches

We're subject to the Notifiable Data Breaches (NDB) scheme. If we ever experience an eligible data breach likely to result in serious harm, we will notify both the Office of the Australian Information Commissioner (OAIC) and the affected clinic owners in line with our obligations under the Privacy Act 1988 (Cth). We test our incident-response process regularly.

What we are not

- **We are not a clinical decision-support tool.** The AI is for business and operational questions about your clinic. It will refuse clinical, diagnostic, or treatment questions. This is by design and is reinforced in every prompt.
- **We are not your bookkeeper or accountant.** The reports help you spot trends and risks; they don't replace professional advice on tax, payroll, or compliance.
- **We are not your privacy officer.** Your obligations as the data custodian for your patients remain yours; we are a third-party processor under your instruction.

Australian regulatory framework — short version

We comply with, or are designed around, the following:

- Privacy Act 1988 (Cth) and the Australian Privacy Principles (APPs 1–13).
- Privacy and Other Legislation Amendment Act 2024 (Cth) — including the forthcoming Automated Decision-Making transparency provisions effective 10 December 2026 (we are designing for these now).
- Health Records and Information Privacy Act 2002 (NSW) — for clinics in NSW.
- Healthcare Identifiers Act 2010 — we don't touch IHIs.
- My Health Records Act 2012 — we don't touch MHR data.
- Notifiable Data Breaches scheme — we're enrolled.
- The National AI Centre's Guidance for AI Adoption (October 2025) — six essential practices treated as our internal governance standard.

> **Questions or concerns?**
>
> Email contact@kookaburra.health for any privacy or security question — we read every message.
>
> You can also take it up with the regulator directly: oaic.gov.au · 1300 363 992.

Operator: Principal Podiatry Pty Ltd · ABN 19 615 606 347 · Registered in Queensland, Australia

This page is a plain-English summary. Our full Privacy Policy is the legally binding document. If anything here conflicts with the policy, the policy controls.