Hakea Care

Security & privacy

A short summary for management, IT and compliance teams of how we look after the care records our customers trust us with.

Where data is stored

Hakea Care runs on **Decided by our hosting team**. All customer data is stored in the **Decided by our hosting team** region.

The database, file storage (voice recordings, uploaded documents, report PDFs) and backups are all kept in that same region.

Encryption

- Data travelling between your browser and Hakea Care is encrypted with TLS 1.2 or higher.
- The database, stored files and backups are encrypted at rest.
- Secrets such as email server passwords, webhook secrets and integration keys are encrypted again with a separate key that only the application holds.
- File links are private and expire after a few minutes.

Who can see what

- Every person has a role: support coordinator, provider, support worker, participant or nominee. What each role can see is set per customer in an access matrix.
- Participants are only visible to their own coordinators and the providers working with them.
- Workers see the details they need for their shifts, nothing more. Providers never see other providers' notes.
- Administrators must use two-step sign-in (MFA).

Customer data separation

Every record is tagged with the customer it belongs to. On top of the application's own checks, the database itself enforces the separation with row-level security, so one customer's data can't be read from another customer's account.

Audit trail

- Every view, export, edit and sign-off is logged with who did it, when, and from where.
- The audit log can't be changed or deleted – not even by our team.
- Customers can filter and export their own audit log at any time.

Records retention

- Notes, reports and incidents are kept for 7 years by default. Each customer can choose 5, 7 or 10 years.
- Voice recordings are deleted after the period the customer chooses (30, 90 or 365 days), once the note text is saved.
- Users can't delete records. Data is deleted on request as set out in the customer contract.

AI use

- Hakea Care uses **OpenAI** through Hakea Care's own business account. Customers don't need their own AI account. OpenAI's servers are outside Australia.
- Data sent to OpenAI is **not used to train AI models**.
- Only the note text is sent – never NDIS numbers, addresses, dates of birth, email addresses or phone numbers.
- AI only runs when the participant (or their nominee) has given consent. Without consent, notes and reports are written by hand.
- Every sentence the AI writes in a report links to the note it came from, so it can be checked. Nothing is shared until a support coordinator has checked the sources and signed the report off.

Consent

- Consent covers three things separately: AI help, voice recordings, and sharing notes with providers outside the platform.
- We record who gave consent, when, which version of the consent text they saw, and what they agreed to.
- Consent can be withdrawn at any time. AI, voice and sharing stop straight away; existing notes are kept.

Reliability and backups

- The database is backed up every day, with point-in-time recovery.
- Stored files are versioned, so an accidental change can be undone.
- We monitor the service and are alerted to errors, failed deliveries and repeated failed sign-ins.

Incident response

If we suspect a data breach we act straight away: we contain it, find out what happened and who is affected, and fix the cause. We tell affected customers promptly and help them meet their obligations under the Notifiable Data Breaches scheme, including notifying the Office of the Australian Information Commissioner and affected people when required.

Compliance roadmap

- Designed to meet the Australian Privacy Principles.
- Supports NDIS Practice Standards record-keeping: complete, dated, signed and unchangeable records.
- An independent penetration test is done before go-live.
- ISO 27001 and SOC 2 certification are planned.

Contact

Questions about security or privacy, or want to report a problem? Email parth.rupareliya@9series.com.