

Security and data handling

Cohearo records and transcribes on your device. This page explains what stays there, what cloud features send to our services, and how we protect that data.

Version 0.2.0

Recording stays on your device

Audio recording, transcription and speaker identification run locally in the desktop app. Your recordings are not uploaded to Cohearo for transcription or AI enhancement.

The voice embeddings used to distinguish speakers also stay on your device. If you sync speaker profiles, their identifiers and the names you assign to them can sync; the voice embeddings do not.

You choose when to use cloud features

In local mode, transcripts are stored on your device. They are not automatically uploaded when you reconnect or switch to cloud mode.

Cloud features use transcript text:

- **AI enhancement:** when enabled, transcript text is sent to our backend and then to our AI provider to generate the result.
- **Cloud sync:** transcripts sync to your account so you can access them through Cohearo's cloud features.
- **Sharing and integrations:** sharing content or authorizing an integration, such as an AI assistant connected through MCP, can make that content available to the people or service you authorize. Their handling of content is separate from Cohearo's AI enhancement processing.

Using an account also involves sign-in, billing and service-usage data. Diagnostics and analytics are described in our Privacy Policy, including the controls available to you. These are separate from audio recording and transcription.

AI processing and zero data retention

We use OpenRouter to route AI enhancement requests. **Zero data retention is enabled on our OpenRouter account**, restricting routing to endpoints that OpenRouter identifies as meeting its zero-retention policy for request content.

This setting concerns the content sent for AI processing. It does not delete transcripts you choose to store in Cohearo, or account, billing and usage records needed to operate the service. It also does not govern an external AI assistant you connect separately.

For the provider's definition and scope of this control, see OpenRouter's zero data retention documentation. Our Privacy Policy provides further information about service providers and personal data.

Storage and protection

Cohearo's production transcript storage is hosted on Amazon Web Services in São Paulo, Brazil. This storage location does not mean that all service providers process data in Brazil: external AI processing and other supporting services may operate elsewhere.

We encrypt traffic in transit and use encryption at rest for our production database and object storage. These protections are not end-to-end encryption: our services process transcript text to provide the cloud features you request.

Access controls restrict account and organization data to authorized users. Administrative functions require additional authorization, and administrator sign-in includes a second verification step. Our public API also uses edge filtering and rate limits to help reduce abusive traffic.

Security review

In August 2026, we conducted an internal application-security assessment using test accounts within and across organizations. It covered access controls and selected authentication, input-handling and integration scenarios in our development environment. The issues identified in that assessment were fixed before it was closed.

This was an internal review, not an independent penetration test or certification. Its findings apply to the version and scenarios assessed; they are not a guarantee that every vulnerability has been found. Cohearo has not been certified against SOC 2 or ISO 27001.

Questions and reporting concerns

For retention, deletion, your privacy choices and information about service providers, read our Privacy Policy.

To ask a security question or report a suspected vulnerability, contact contact@cohearo.com. Describe the issue and how to reproduce it without including passwords, API keys or other people's private content.