Astralcyte
NOTES

Client Information for Astralcyte Notes

Your clinician may use Astralcyte Notes to help prepare notes about your session. This handout explains how the program handles your information and respects your privacy.

What does it do?

The program transcribes a written transcript of the session, and uses a local AI running on your clinician's computer to draft a summary note. Your clinician checks the draft for mistakes and missing information before using it in your record.

Where does my information go?

Nowhere. Transcription and note drafting run on your clinician's device, and can be run entirely without internet. The program does not send your session audio, transcript, or notes to Astralcyte or any online AI service for processing.

How does Astralcyte Notes keep my data secure?

Your records are encrypted on your clinician's device. Unlocking them requires the clinician's passphrase or recovery key. Encryption makes the stored records unreadable without the key needed to unlock them.

Temporary audio is also encrypted. Once it has been transcribed, the program destroys its encryption key and deletes the audio. There is no saved recording of client discussions.

The vault locks when the application closes or the computer's user session locks or signs out. Your clinician can also configure an inactivity lock. Astralcyte has no copy of the vault key and no backdoor. If both the passphrase and recovery key are lost, the vault cannot be recovered.

Is a recording kept?

Audio is stored temporarily in encrypted form for transcription and recovery if a session is interrupted. Once audio is transcribed, the program destroys the audio key and deletes the encrypted audio. The audio cannot be played back or exported from the program.

What is kept after the session?

Notes are stored in an encrypted vault on the device. The program keeps the transcript by default, though your clinician can choose to delete it after approving the note.

Your clinician can copy notes into your clinical record and make encrypted backups. Ask where your records and backups are stored, who can access them, and how long they are kept. These choices depend on the practice.

Before your session

Ask your clinician to explain how they plan to use the program. Tell them if you do not want it used, or if you want it stopped during the session, and discuss how they will take notes instead. You can also ask what happens to information already captured if you change your mind.

For questions about your records or a privacy concern, contact your clinician or the practice. More about the software is available in Astralcyte's Privacy Policy and Security Policy.

Can you give me more technical details?

Clinical records are stored in a SQLCipher-encrypted database with a randomly generated 256-bit key. SQLCipher encrypts database pages using AES-256-CBC and authenticates them with HMAC-SHA512 to detect tampering or corruption.

Argon2id derives a separate salted wrapping key from the clinician's passphrase. That key protects the database key using XChaCha20-Poly1305 authenticated encryption. Argon2id makes repeated passphrase guesses costly in computing time and memory.

Temporary audio also uses XChaCha20-Poly1305 authenticated encryption, with a separate random key for each session. Once a complete transcript is saved, the program destroys the stored audio key and deletes the encrypted audio.

While the vault is unlocked, the program must decrypt information in memory to use it. SQLCipher's memory-security setting is enabled to wipe its allocated memory when it is freed.