

The data never leaves the building.

Conversation Simulator for regulated-sector training: a privacy architecture you can verify, mapped to HIPAA and FERPA postures in plain language.

The problem, in one line

The conversations institutions most need to rehearse - a diagnosis, a disclosure, an IEP meeting, a Title IX intake, a use-of-force debrief - are exactly the ones they cannot send to someone else's server. Every funded competitor in conversation practice is cloud SaaS, priced per seat. For a regulated buyer that is a procurement wall, not a feature gap.

The architecture: local by design, not by policy

Conversation Simulator has no server. Every part of the system runs on the practitioner's own machine:

- **On-device language model.** The AI character runs locally (llama.cpp). Prompts and replies never leave the machine.
- **On-device speech.** Speech recognition (whisper.cpp) and the character's voices are synthesized locally. Audio is never uploaded.
- **On-device storage.** Every transcript and score lives in a SQLite database on your own disk - never in a vendor's cloud.
- **No account, no telemetry, no subscription.** There is nothing to log in to, because there is nothing to connect to.

The receipt: a claim you can check before you buy

Trust you cannot verify is just branding. This you can verify. One command runs a full scripted conversation end to end and fails loudly if any subsystem so much as attempts an outbound connection:

```
npx convsim offline-smoke-test packs/official/job-interview-basic
```

Run it on your own hardware, on your own network, before a dollar changes hands. The no-egress claim is a test you can execute, not a promise you take on faith.

What this means for compliance (plain language)

The following describes the architecture in the language of two common postures. It is descriptive, not legal advice - see the note at the foot of this document.

- **HIPAA posture.** Protected health information a trainee speaks aloud stays on the device. Nothing is transmitted or stored off-site, so there is no cloud processor to add to a Business Associate Agreement and no off-site transcript store to breach. The most defensible posture for ePHI is the one where the data never leaves the covered entity's control.
- **FERPA posture.** Student education records - including oral-exam performance and any recording of it - never leave institutional control. There is no third-party 'school official' receiving the data, because there is no third party receiving the data at all.

- **Data minimization by architecture.** The system cannot exfiltrate what it never sends. Minimization stops being a setting an administrator has to get right and becomes a property of the design.

What you own, and how content is governed

- Commissioned scenario packs are delivered as YAML you own outright. The engine is Apache-2.0. There is no lock-in, because there is no server to be locked into.
- Two immutable safety rules ship in every scenario, from every author, and no configuration can weaken them. Commissioned work is governed by a published content-review policy that makes those rules contractual.
- The built-in Creator Workbench validates every pack against a published quality bar before it ships.

The offers

- **Scenario Pack Commission - \$6,500, 2-3 weeks.** Five to eight authored, safety-reviewed scenarios with rubrics and debrief logic, delivered as YAML you own. Sized to slip under a \$10k discretionary threshold.
- **Private Practice Pilot - \$12,000, 6 weeks.** A commissioned pack, a branded deployment, a facilitator guide, and pre/post measurement design for one cohort of up to 50 practitioners - so the cohort's improvement is a number, not a vibe.

Both land under a single year of a 50-seat cloud contract (roughly \$18k-\$30k at market per-seat rates) - and unlike that contract, they ship with zero data egress. You buy an asset you keep, not a subscription that reads your people.

One line for the procurement file: there is no server, and you can verify it with one command.

About this document

This one-pager describes the architecture of Conversation Simulator and is provided for information only. It is not legal, compliance, or regulatory advice, and it is not a warranty or certification of compliance with HIPAA, FERPA, or any other law or standard. Whether a given deployment satisfies a given obligation depends on your institution's own policies, configuration, workforce practices, and controls. Map this architecture to your obligations together with your own privacy, compliance, and legal counsel.

Talk to the studio: hi@outrightmental.com - outrightmental.com/services/conversation-systems/