AI in clinical work, without the breach headline.

$7.42M

Average cost of a healthcare data breach, the costliest of any industry studied.
Source: IBM Cost of a Data Breach Report, 2025.

THE EXPOSURE

- **Shadow AI is already in the clinic.** Notes and chart data get pasted into AI tools no one approved, alongside live patient records.
- **PHI leaves the boundary unrecorded.** Once a prompt reaches an outside model, PHI has crossed, with no record and no enforced policy.
- **Nothing to produce on request.** An OCR inquiry or 42 CFR Part 2 review asks what the AI saw. No record, no answer.

WHAT CHANGES WITH VERILLIAN

- **Sensitive content is contained at the device.** PHI detection redacts or blocks before content reaches a provider. Detection is best-effort; the sentinel fails closed.
- **You hold the keys.** The record is encrypted under your own key on a server that stores ciphertext it cannot read.
- **Proof you can produce and verify.** Every captured interaction is signed on the device and hash-chained into an append-only, tamper-evident record, verifiable mathematically.
- **No workflow change.** A sentinel governs any tool that reaches a provider over HTTPS, with no per-tool integration.

Built for HIPAA and 42 CFR Part 2. The control sits on the device, so PHI you do not send cannot be breached, and audit content stays under your own key, aligned to HIPAA's six-year retention.

To start a pilot, name a sponsor and a technical contact, and we will scope the first week in your environment, on your own infrastructure, under your own keys.

hello@verillian.ai