Verillian for Healthcare

HIPAA, HITRUST, 42 CFR Part 2

Clinicians recover hours a day from AI. The records they work near are the most regulated in the country. Verillian lets health systems use frontier models while keeping protected health information inside the boundary and every interaction on the record.

$9.77M

Average cost of a healthcare data breach, the costliest of any industry for fourteen years running. IBM Cost of a Data Breach Report, 2024.

WHAT'S AT STAKE

When clinicians paste notes, labs, or chart data into AI tools, protected health information can cross the boundary to an outside provider with no record that it happened. Under HIPAA, each exposure carries breach-notification, OCR enforcement, and per-record penalty exposure. With nothing in place, an organization cannot prove what left, who sent it, or that policy was enforced, which is exactly what an audit or breach investigation demands.

HOW VERILLIAN ANSWERS

Keep PHI inside the boundary	Sensitive-data detection redacts or blocks SSNs, medical record numbers, and other PHI before a request ever leaves the device, so protected health information does not reach an outside AI provider.
Govern every AI tool, not just the sanctioned ones	A sentinel governs any tool that speaks HTTPS to a provider, with no per-tool integration, and surfaces shadow AI so unapproved tools touching patient records are discovered rather than silently in play.
Put every interaction on the record	Each interaction is signed on the device and hash-chained into an append-only, tamper-evident record, retained to align with HIPAA's six-year requirement. Non-repudiable evidence of what was sent and that policy held.
Deny by default, fail closed	Policy is enforced at the moment of execution. With no valid policy or an audit-pipeline failure, AI traffic stops, so the system cannot quietly leak PHI when controls are degraded. Built for HIPAA-regulated environments, with ciphertext stored under your own key.

Start a pilot. **verillian.ai**

Source: https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs