



FOR LEGAL

AI on client work. A record that answers to privilege.

Your clients did not choose to have their matters read by a model, and your duties do not pause because a tool is useful. Verillian governs AI on your own hardware, screens identifiers at the device, and seals a record only the firm can read.

WHERE THE EXPOSURE SITS IN A FIRM



Drafting, at deadline

An associate with a deposition in four hours, a paralegal on the ninetieth document. AI arrived as one more browser tab.



Confidences that travel

Privilege and work product move with the material, whichever tool it is pasted into, at whatever hour.



Someone will ask

Outside counsel guidelines now ask which AI tools touched the matter, and increasingly reserve a right to audit the answer.

WHAT THIS MAPS TO



Client confidentiality

Screened at the device, before anything reaches a provider.



Outside counsel guidelines

Which tools were used, by whom, on which matters, from a record.



Client audit rights

An export the client can verify without reading your content.



Work product

Deny-by-default policy signed and distributed to every device.



Bar and ethics duties

Competence and supervision, evidenced rather than asserted.



Regulated clients

Financial and health clients bring their own controls.

Aligned, not independently certified. Your firm holds the duty.

What the layer does on a firm's device

Govern AI on matter data

Tool calls on the Anthropic API format are decided on the device against deny-by-default policy before they run; other captured calls are recorded.

Screen data before it leaves

The identifiers it catches are stripped on the device on a best-effort basis before a prompt or file leaves the endpoint.

Answer the questionnaire

Show, per captured interaction, what AI was allowed to do, what it was not allowed to do, and what policy changed.

Self-hosted, no vendor custody

Prompts, files, and decisions stay on your infrastructure. There is no Verillian cloud in the path.

Keep the whole turn

Where a log says something happened, the record keeps the interaction: what was asked, what it did, and the ruling it met.

Rules per practice group

Litigation does not need the same policy as transactional. Each group carries its own declared rules, applied the moment you set them.

What a firm is buying



Deny by default

Anthropic-format tool calls you haven't allowed are refused.



Screened on device

Flagged identifiers replaced before a prompt leaves.



Hash-chained record

Every captured interaction, sealed and verifiable.



Your keys only

Encrypted under keys only the firm holds.



Five switches

Four scoped stops, plus a halt across every device.



Runs air-gapped

On-prem, private cloud, or fully air-gapped.

The record a client audit can meet

TIME	USER	MODEL	DECISION	CONTENT	CHAIN
17:12:04	associate@firm.example	claude.ai	 REDACT	REQUEST summarize the client intake	b74e...3c19
17:12:06	associate@firm.example	claude.ai	 ALLOW	REQUEST build a timeline	carries 1a06...d8f2
17:12:22	associate@firm.example	claude.ai	 BLOCK	REQUEST copy the matter folder out	carries 9c31...402b

Illustration of the record format. Each entry carries the hash of the one before it, so change any entry and the chain breaks, and the break is plain to see.

What a client's auditor can check



Which tools touched the matter

Each entry is signed by the device it came from, so use traces to a person, a tool, and a time.



An answer to the guideline

When a client asks whether AI touched their work, you produce the sealed turn rather than a policy memo.



No vendor in the data path

Prompts and records stay in your own environment, so there is no vendor cloud for a client to worry about.



Which policy version ruled

Policy is authored once and distributed to every enrolled device, with a record of which version decided any given action.



Keys only the firm holds

The record is encrypted under keys only the firm holds. Verillian never receives your prompts, your files, or your record.



Retention on your schedule

The record of every captured interaction is kept on your infrastructure for as long as your retention schedule says.

Deployment reality

Endpoints

Mac, Windows, and Linux today, deployed like the rest of your endpoint software. Policy is scoped by group, not by person.

The admin server

Runs where you choose: on-prem, private cloud, or fully air-gapped, so it fits the boundary your matters already live inside.

The limits, stated

Redaction is best effort, and matter numbers are not a detected type. Tool blocking ahead of execution runs on the Anthropic API format today.

Let them use it, and be able to show what it did.

Book a demo and we'll run it on the drafting your associates actually do, then hand you the sealed record to test. No vendor discharges a professional duty: Verillian supplies the enforcement point and the evidence.

hello@verillian.ai