

LitAxis Security Overview

Updated October 14, 2026 | litaxis.app/security

LitAxis is case management and intake software for plaintiff law firms. A firm's data is some of the most sensitive there is: medical records, settlement money, privileged strategy. This overview lists the controls in place today, the agreements behind them, every company that processes firm data for us, and what isn't in place yet.

Agreements and data location

- **Business associate agreement with AWS (in place).** LitAxis has a signed business associate agreement (BAA) with Amazon Web Services, active since October 14, 2026. It covers AWS's HIPAA-eligible services, which host the LitAxis application, its database and your documents.
- **A BAA for your firm (in preparation).** Our business associate agreement for firms is being finalized. Ask us and we'll tell you where it stands.
- **Data stays in the United States (in place).** Firm data is stored in AWS's US West (Oregon) region. Drafting, chronology and analysis AI runs on Amazon Bedrock in US regions, and the companies that make the models don't receive your data.
- **Independent security audit (not yet).** LitAxis hasn't completed a third-party security audit. When it has, the report will be listed here. Until then we show no badges, and we're glad to walk your team through every control in detail.

Controls in place

- **Firm-by-firm isolation.** Every query is scoped to your firm in the application, and Postgres row-level security enforces it again in production.
- **Encrypted, stored and moving.** The database, document storage, secrets and call recordings are encrypted with AWS KMS customer-managed keys, with rotation on. Connections are HTTPS-only, with Strict Transport Security.
- **Integration tokens sealed.** Access tokens and API keys for the ad, accounting, chat and data services you connect are encrypted (AES-256-GCM) before they are stored.
- **Ethical walls beyond the screens.** Record-level screens apply in the app, the API, the MCP server, custom Canvas screens and Slack commands — not just the main screens.
- **Multi-factor sign-in.** Passkeys (recommended) or authenticator apps, one-time recovery codes, and remember-this-device for 30 days. The firm owner can require a second factor for everyone, for owners and admins, or leave it optional — with a separate setting for the client portal.
- **Directory provisioning (beta).** Connect your identity provider over SCIM 2.0 to add, update and deactivate LitAxis users from your own directory. LitAxis stores only a hash of the connection token.
- **Roles you define.** Configure what each role can see and do, per firm.
- **Tamper-evident audit trail.** Changes and sign-ins go into a hash-chained log. Database triggers block ordinary edits and deletes, and a one-click check in settings verifies the chain is intact.
- **API keys done carefully.** Stored only as hashes, limited to the scopes you grant, acting as the person who created them, and rate-limited.
- **Outbound calls fenced.** Webhooks and integrations can't be pointed at internal addresses (SSRF protection with IP pinning).
- **Backed up and versioned.** The database keeps continuous backups with point-in-time restore, and stored documents keep their earlier versions, so an accidental change or deletion can be recovered.
- **Built on AWS.** CloudFront, Lambda, Aurora PostgreSQL and S3. Drafting, chronology and analysis AI runs on Anthropic's Claude through Amazon Bedrock.

AI guardrails

- AI chronology entries that can't quote their source word for word are dropped, not shown.
- Case valuation says how many of your settled cases it compared against, and their range — or that there aren't enough.
- Suggested next steps on a matter never send, file or execute anything on their own.
- AI Jobs ship switched off. Their AI steps wait for a person to approve or run them, and drafted letters wait for review.

- The client portal's AI answers only from client-safe case information, and is instructed to hand legal-advice questions to your team.

Subprocessors

- **Amazon Web Services (AWS).** Hosting, database, document storage, AI models (Anthropic's Claude on Amazon Bedrock), text recognition, the phone system, email, sign-in, encryption keys and logs. Data it receives: all firm data, including medical records, documents, call recordings and AI requests. Location: United States.
 - **ElevenLabs.** The AI voice agent that can answer a firm's intake calls, and natural voices for phone menus. Data it receives: what callers say on intake calls, and the call scripts a firm writes. Location: Not yet confirmed.
 - **Twilio.** Phone numbers that carry intake calls to the AI voice agent. Data it receives: call audio and callers' phone numbers on intake calls. Location: Not yet confirmed.
- Services your firm connects with its own account — such as Microsoft 365, Slack, your ad accounts or your identity provider — receive data only once you connect them, under your firm's own agreement with that company.

Not available yet

- **Single sign-on.** Per-person sign-in through your identity provider (SAML / OIDC).

Contact

Questions, a security review, or a vulnerability to report: hello@litaxis.app. If you think you've found a vulnerability, tell us before anyone else and we'll work with you on it. The latest version of this overview and the subprocessor list are always at <https://litaxis.app/security>.