

CaseRead security summary

How CaseRead keeps a law firm’s client files private.

September 29, 2026

SOC 2 aligned Every control on this page is live in CaseRead today.

Controls live today

A database schema for every firm

Every firm gets its own database schema the moment it signs up, with its own document tables, search index and row-level security. Other firms’ searches can’t reach your vault, and vault search picks the schema from the signed-in lawyer’s own account, never from the request.

A firm activity log

Firm admins see who viewed, downloaded or exported a document, who was denied one, and every role change, invite and two-factor change, and can export the log to CSV. A private document’s title stays hidden from anyone who can’t open it.

No training on your data

CaseRead runs no model training or fine-tuning on your data, and our AI providers’ commercial terms exclude it from their training.

Encrypted in transit

TLS encryption in transit, with HTTPS enforced on every page.

Every citation checked

Every citation checked by the Hallucination Shield: does the source exist, and does it support the claim.

Rule 1.6 and ABA Formal Opinion 512

ABA Formal Opinion 512 (July 29, 2024) says a lawyer needs the client’s informed consent before entering client information into a self-learning AI tool, and that boilerplate in an engagement letter is not enough.

Your Rule 1.6 confidentiality duty, mapped to CaseRead’s controls.

Keep your firm’s client files away from other firms	A database schema for every firm
Limit who inside the firm sees a matter	Private by default
Stop a stolen password from opening the account	Two-factor sign-in
Know who opened, downloaded or exported what	A firm activity log
Keep client information out of AI model training	No training on your data
Erase a client’s files when the matter ends	Instant, verifiable purge

ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion 512 (July 29, 2024). Read September 28, 2026.
https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf

Questions: info@caseread.ai · www.caseread.ai/security

Two-factor sign-in

Every CaseRead account can turn on two-factor sign-in with an authenticator app, with recovery codes and a list of signed-in sessions you can end. A firm admin can require it for everyone in the firm.

Instant, verifiable purge

Delete a project and CaseRead erases its documents, files, versions, AI conversations, memory, workflow results, monitors, share links and upload links, across every CaseRead store and for every member of the firm, in one step. We keep a content-free record that the purge ran: counts, never names.

AES-256 encryption at rest

Our database host, Supabase, encrypts everything it stores for us at rest with AES-256. CaseRead encrypts Google and Microsoft connection tokens and share-link passwords again with AES-256-GCM.

Private by default

New projects are private to the lawyer who creates them.

Hosted in the US

Database and files hosted in the US (AWS, via Supabase).