CounselCore: In■House Sovereign AI for Law Firms

Overview

CounselCore is a non■cloud, in■house AI system that allows attorneys to use modern AI across the firm’s prior matters without moving a single client document to the public cloud.

It is designed for firms that want the efficiency and insight of AI, but cannot accept the legal and evidentiary risk of sending privileged material to external AI providers.

CounselCore: In■House Sovereign AI for Law Firms

Why in■house instead of cloud AI?

1. Attorney–client privilege

When privileged material is processed by third■party cloud systems, opposing counsel can argue that privilege has been weakened, waived, or that the scope of privilege has become unclear. Even if the argument fails, it creates an issue that must be briefed and defended.

Keeping AI systems in■house allows the firm to maintain that all substantive processing occurs within its own ethical and privilege boundary.

2. Discovery and chain of custody

Cloud AI systems create additional logs, caches, and backups across multiple vendors and regions. Each can become a potential discovery target and complicate the chain■of■custody narrative.

With an in■house system, the firm can account for exactly where data lives, how it is processed, and which systems must be addressed in discovery.

3. Confidentiality and ethics obligations

Client outside counsel guidelines, regulatory frameworks, and professional responsibility rules often restrict where and how confidential information may be stored or processed.

In■house AI makes it straightforward to say, “We do not send your matters to external AI providers. All processing remains inside firm■controlled systems.”

4. Institutional knowledge as both evidence and advantage

Decades of briefs, memos, emails, transcripts, and research are both potential evidence and a core competitive advantage. Treating that history as training fuel for vendor models exposes a central firm asset to long■term strategic risk.

CounselCore lets the firm use AI over that history without ceding ownership or control.

What CounselCore is

• A sovereign, in■house AI layer deployed on firm■controlled infrastructure.

• A retrieval■augmented system that grounds every answer in the firm’s own documents.

• A permissions■aware interface for attorneys to query prior matters, filings, research, and correspondence.

• A system that never calls public AI APIs and never sends client data to the cloud.

CounselCore: In■House Sovereign AI for Law Firms

How it works (high level)

1. Ingest and index documents from your DMS, file shares, and archives with matter■level metadata.

2. Create vector and text indexes stored entirely inside your infrastructure.

3. Allow attorneys to query the system through a secure, authenticated interface.

4. Return answers that are explicitly tied to underlying documents, with citations and links to the original sources.

5. Log usage in a way that can be reviewed internally and, if needed, explained to a court or regulator.

Who it is for

• Firms handling matters where privilege, regulatory scrutiny, or client instructions make cloud AI usage difficult or unacceptable.

• Firms that view their historical work as a strategic asset and are unwilling to expose it to third■party training or infrastructure.

• Leadership teams that want to make AI a standard capability, but only on terms they can defend professionally and ethically.

Key talking points for clients

• “We use AI only inside the firm’s own systems. Your matters are never sent to external AI providers.”

• “Our AI capability is grounded in our own prior work, which is subject to the same controls as the rest of your matter file.”

• “If asked how we used AI on your matter, we can explain the process and systems clearly and defensibly.”