TheFormTool LLC

The Ownership Illusion: Why Client Data in the Age of AI Demands New Rules

It's time for lawyers, law firms, bar associations, and others working with confidential information or subject to CCPA, HIPAA, or GDPR to look past hardware and encryption to address the basic issue: after data is shared with the cloud, who actually owns and controls it?

Executive Summary

Despite well-meaning guidance from regulators, the legal profession is standing on unsteady ground. The rapid adoption of cloud-based services and AI-enhanced legal tools has made it easier than ever to compromise the confidentiality, privilege, and integrity of client data — not through carelessness, but by design.

This white paper outlines what TheFormTool has learned through extensive research, how guidance from multiple authorities has attempted to steer lawyers toward compliance, and why these attempts have missed the mark. The central conclusion is blunt: absent enforceable control and clear ownership, true client confidentiality cannot be guaranteed.

1. The Missing Layer in Legal Ethics

Cloud storage, large language models, and "smart" features in legal software all have something in common: they are black boxes to the lawyers who use them. Vendors routinely collect, analyze, and sometimes retain data shared with them, whether under a click-through license agreement or without any meaningful disclosure.

While regulators and ethics committees have focused on encryption, cybersecurity, and disclosure, these efforts treat the symptoms but ignore the disease.

The problem isn't the method of transmission. It's that when a lawyer shares client data with an external system — especially one using AI — they relinquish ownership and control. Confidentiality and privilege are no longer enforceable once client data becomes third-party training material, is retained in backend logs, or is reused for model tuning.

2. "Reasonable Efforts" Are No Longer Enough

Most current guidance falls under the umbrella of "reasonable efforts," typically tied to encryption and basic security hygiene. Consider these examples:

- ABA Model Rule 1.1 cmt [8]: Lawyers must understand the "benefits and risks associated with relevant technology."
- ABA Formal Ethics Op. 477R (2017): Urges the use of secure communications but fails to explore consequences of external processing.
- OSB Formal Opinion No. 2011-184: Warns that even anonymized "hypotheticals" can violate client confidentiality.
- NYSBA Report (2024): Suggests lawyers may want to disclose AI use in engagement letters — a strikingly soft recommendation.

- Texas Opinion 705: Lawyers must understand and take precautions regarding generative AI, its data usage and storage risks, and its potential to expose privileged information.

These statements place the burden entirely on the lawyer to ensure protections — even when such protections may be technically impossible.

3. What Lawyers Don't Know Can Hurt Everyone

In many cases, lawyers are unaware of how third-party systems handle their data:

- Do vendors use subcontractors?
- Where is the data stored?
- Is it used to improve AI models?
- Is it retained for future analysis?
- Can client data be removed on request?

A recent example: Microsoft Azure's OpenAI service allowed internal employees to view prompt and response logs as part of its abuse monitoring system. There's no reason to believe this is an isolated case.

From Texas Bar Guidance:

> *"Sharing sensitive client information with non-enterprise AI platforms, especially general-purpose tools that may lack robust data security or confidentiality guarantees, risks unauthorized disclosure. This violates the attorney's strict duty of confidentiality (Tex. Disciplinary R. Prof. Conduct 1.05)."*
>
> *"By their very nature, many generative AI tools invite a 'conversation' in which the lawyer... will explain relevant facts, legal theories, and arguments. These exchanges could, if nothing else, expose the lawyer's privileged mental impressions to the generative AI tool."*

This risk is even more pronounced in document automation work, where tools must incorporate detailed, often sensitive client information — from estate plans and health directives to divorce settlements and merger agreements. These datasets, when shared via cloud-based platforms, become high-value targets and lose enforceable protections.

The problem is not just theoretical. The first significant breach of privileged legal data will be catastrophic. The second will be existential.

4. Bar Opinions Are Behind the Curve

Recent ethics opinions and white papers — including those from the ABA, NYSBA, and OSB — generally sidestep the ownership and control issue. They assume that client confidentiality can survive a trip through the cloud, provided the right checkboxes are ticked.

But the truth is that lawyers cannot effectively audit the behavior of proprietary AI vendors, and no checklist can overcome that barrier. Without authority over the vendor's practices and guarantees of non-retention, data shared into these systems is no longer truly private.

5. An Unfulfillable Standard

Lawyers are expected to evaluate their vendors' behavior in storing, using, and transmitting client data. But what if that evaluation is impossible?

- License agreements often include disclaimers and changeable terms of service.
- Some vendors refuse to disclose whose AI systems power their features.
- Others repackage models from OpenAI, Google, Anthropic, or Meta.

This creates a fundamental mismatch between the obligations of the lawyer and the realities of the technology.

6. The Only Ethical Default: Don't Share

At TheFormTool, we've reached the conclusion that ownership and control of client data must be the baseline for ethical law practice. Everything else is built on sand.

In the absence of enforceable assurances that lawyers maintain full authority over their data, including its retention, reuse, and analysis, the only defensible position is not to share it at all.

Offline tools, local data storage, and controlled document automation — without cloud transmission, without third-party analytics, and without persistent external access — are the only current way to ensure that client information remains truly privileged and confidential.

Appendix: Supporting References

- ABA Model Rule of Professional Conduct 1.1, Comment [8]
- ABA Formal Ethics Opinion 477R (2017)
- ABA Formal Ethics Opinion 512 (2024)
- NYSBA AI Task Force Report (April 2024): https://nysba.org/app/uploads/2024/02/Task-Force-on-AI-Report-final.pdf

- Oregon State Bar Formal Opinion 2011-184
- Oregon State Bar Formal Opinion 2025-205 (AI Tools)
- Microsoft Azure OpenAI Employee Access Disclosure (2024)
- ·OpenAI Federal Court Order on User Log Preservation (2024)
- Texas Bar Ethics Opinion 705 (2024): https://www.legalethicstexas.com/resources/opinions/opinion-705/
- Texas Bar Practice: "AI in Your Law Practice" https://blog.texasbarpractice.com/ai-in-your-law-practice-tips
- Texas Bar Practice: "Liability and Risk Management" https://www.texasbarpractice.-com/liability-and-risk-management/

Other resources:

https://theformtool.com/lp/security/

AI, Privacy, and Legal Ethics: Lessons from 23andMe and the Copyright Wars

Legal Privilege, Cloud AI and the Ethics Gap in Document Automation

TheFormTool LLC

www.theformtool.com
info@theformtool.com