

AI AND CLIENT CONFIDENTIALITY

Three Questions to Ask Every AI Tool Your Firm Uses

Florida Bar Ethics Opinion 24-1 (January 2024) says lawyers may use generative AI, and that protecting client confidentiality means checking each tool's policies on **data retention**, **data sharing**, and **self-learning**. Here are the questions to ask, one tool at a time.

First, make a list. Write down every AI tool your team used this month, like ChatGPT, Copilot, or Gemini. Next to each one, note whether people sign in with a firm account or a personal one.

1 Retention

Does it keep what we type?

- ☐ Does the tool save prompts and uploaded files?
- ☐ How long does it keep them, and can we delete them?
- ☐ Is the same setting in place on every account at the firm?

2 Sharing

Who else can see it?

- ☐ Do the terms allow the vendor to share what we enter with third parties?
- ☐ Can the vendor's staff review prompts or files?
- ☐ Do personal accounts follow different terms than firm accounts?

3 Self-learning

Does it learn from our data?

- ☐ Are our prompts and files used to train the vendor's models?
- ☐ Is training turned off by default on our plan, or does someone have to switch it off?
- ☐ Who at the firm confirms it stays off after updates?

Can't answer one? Treat it as a gap. Personal accounts and default settings are the first places to look.



WANT A SECOND SET OF EYES?

Get a free, written AI risk summary for your firm.

Brian Butterfield, CISSP, Co-Founder and Chief Security Officer at Microtech, goes through these questions with you on a 30-minute call. Only 10 firms a month.

micro-tech.com/ai-risk-review • 954-327-1001