

FREE PDF GUIDE

AI Ethics and Copilot Readiness for Law Firms

ABA and Texas AI opinions explained

October 2026

24unet.com

Denver (303) 468-5515 | College Station (979) 256-5100 | sales@24unet.com

Can Your Law Firm Use AI With Client Files? Ethics Rules and Copilot Readiness

A 24uNet guide for law firms

Generative AI tools such as Microsoft Copilot can draft, summarize and search faster than any associate. But the ethics rules don't change because the tool is new. The ABA and the State Bar of Texas have both issued opinions on lawyers' duties when they use AI. Older ABA opinions on secure communications and data breaches still apply too. This guide covers what those opinions ask of you, and how to get your Microsoft 365 environment ready before client data goes into an AI tool.

> **Not legal advice.** This guide is general information about ethics guidance as of October 2026. Ethics opinions are advisory, and how they apply depends on your jurisdiction and practice. Confirm your obligations with ethics counsel or your state bar.

What the ethics opinions say

ABA Formal Opinion 512 (July 2024): generative AI

ABA Formal Opinion 512 is the ABA's first guidance on generative AI. It applies existing Model Rules to AI tools.

- **Competence:** lawyers must understand enough about a tool's abilities and limits to use it well, and must check its output.
- **Confidentiality:** before you enter client information into a tool, understand how the tool stores, uses and shares that data. Some tools may require the client's informed consent.
- **Communication:** in some situations, clients should be told how AI is being used on their matter.
- **Supervision:** managing lawyers need policies and training for lawyers and staff, plus diligence on AI vendors.
- **Fees:** billing must be reasonable when AI saves time.

Source: ABA news release on Formal Opinion 512

How 24uNet helps: We vet AI tools before client data goes in. We review where data is stored, whether it is used to train models, who can reach it, and what the vendor's terms say. Then we put the findings in writing so your supervision policy rests on facts.

Texas Ethics Opinion 705 (February 2025)

The Professional Ethics Committee for the State Bar of Texas says Texas lawyers may use generative AI if they meet several conditions. They must understand the tool and protect confidential information. That includes reviewing the tool's terms and data security and training staff. They must also verify the output. The opinion builds on Texas Disciplinary Rule 1.05 on confidentiality. It also builds on the technology competence comment added to Rule 1.01 in 2019. Sources: Opinion 705; Texas Bar Blog summary; Texas Disciplinary Rules

How 24uNet helps: Our security awareness training now covers safe AI use, so your staff training is something you can document. Texas firms can also build this into Lone Star Assurance, our Texas cybersecurity program.

Colorado

Colorado Rule of Professional Conduct 1.6(c) requires reasonable efforts to prevent unauthorized disclosure of, or access to, client information. Colorado Bar Association Formal Opinion 149 addresses security in virtual law practice. Source: CBA Formal Opinion 149. Colorado's AI law for automated decisions (SB 26-189) takes effect January 1, 2027. See the Colorado AG AI page.

How 24uNet helps: For Denver and Colorado Springs firms, we apply the same AI review and Microsoft 365 hardening. We also track Colorado's AI rules as they take shape.

ABA Formal Opinions 477R and 483: the foundation

- **477R (2017):** lawyers must make reasonable efforts to secure client communications. Depending on how sensitive the information is, that can mean encryption or other measures.

- **483 (2018):** after a data breach, lawyers must monitor for it, act to stop it, restore systems, investigate, and notify current clients when their data is compromised. The opinion recommends an incident response plan.

Sources: ABA Law Practice Today on reasonable safeguards; ABA Journal on Opinion 483

How 24uNet helps: We set up Microsoft 365 email encryption and secure file sharing. We also write and test incident response plans and back them with 24/7 managed detection and response, with security analysts reviewing alerts. If a breach happens, our incident response support helps you investigate and work out what to tell clients.

Microsoft Copilot: why permissions come first

Microsoft 365 Copilot works within the permissions each user already has. It can surface any file a person can open, including files they never knew they had access to. That makes old oversharing a real confidentiality risk. A SharePoint site shared with "everyone," a OneDrive link set to "anyone with the link," or a matter folder that never got locked down can all show up in an answer. Ethical walls that exist only on paper won't stop it.

Before rolling out Copilot, a firm should do the following:

1. **Find oversharing.** Review SharePoint sites, Teams and OneDrive for broad sharing, guest access and open links.
2. **Fix permissions by matter.** Limit access to the people working the matter, and enforce ethical walls in the system itself.
3. **Apply sensitivity labels.** Label privileged and confidential content so encryption and access limits travel with the file.
4. **Turn on audit logging.** Keep a record of what Copilot users searched and opened.
5. **Write and train an AI policy.** Cover approved tools, what may be entered, output review and client communication.
6. **Pilot, then expand.** Start with a small group and review the results before a firm-wide rollout.

How 24uNet helps: Our Microsoft Copilot readiness service does exactly this. It covers permissions cleanup, an oversharing review across SharePoint and OneDrive, sensitivity labels, and audit settings. We follow up with staff training. We have also written about a newer risk, prompt injection through external email.

Checklist: how IT supports each duty

Duty	Source	How IT supports it
Competence with AI tools	ABA 512; Texas Op. 705; Texas Rule 1.01 cmt. 8	AI tool review; staff training
Confidentiality of client data	ABA 512; Texas Rule 1.05; Colorado RPC 1.6(c)	Vendor terms review; oversharing cleanup; sensitivity labels
Supervision of lawyers and staff	ABA 512	Written AI policy; approved tools list; audit logging
Client communication	ABA 512	Plain-language AI disclosure support; record of tools used
Secure communications	ABA 477R	Email encryption; secure file sharing; phishing-resistant multifactor authentication
Breach response	ABA 483	Incident response plan; 24/7 managed detection and response; account takeover response

How 24uNet supports law firms

- **Microsoft Copilot readiness:** permissions cleanup, oversharing review and sensitivity labels.
- **24/7 managed detection and response:** security analysts review alerts day and night.
- **Incident response planning and support.**
- **Microsoft 365 security hardening and identity threat detection and response.**
- **Phishing-resistant login and multifactor authentication.**
- **Backup, disaster recovery and business continuity.**
- **Security assessments,** the Security Baseline, and annual external vulnerability scans.
- **Security awareness and phishing training,** including safe AI use.
- **Vendor oversight:** review of breach-notice and data-use terms in IT and AI contracts.
- **Managed IT,** plus Lone Star Assurance for Texas firms.

Talk to 24uNet. Denver (303) 468-5515 · College Station (979) 256-5100 · sales@24unet.com · 24unet.com