USING AI TOOLS IN YOUR PRACTICE

AI Platform Confidentiality & Security: Directive for Legal and DR Professionals

AI Platform Confidentiality & Security: Directive for Legal and DR Professionals

As a legal or dispute resolution professional, your use of Generative AI (GenAI) is governed by stringent ethical duties, particularly the duty of **Confidentiality (ABA Model Rule 1.6)** and the duty of **Technological Competence (ABA Model Rule 1.1, Comment 8)**.

Directive: You must select an AI service tier that guarantees client data will **NEVER** be used for model training or retained in a shared environment.

I. Risk Assessment & Service Tiers: Confidentiality Mandate

Tier	Platform & Plan	Verdict	Why It Matters (Ethical Risk)	ACTION REQUIRED
1. Consumer/Free	ChatGPT (Free / Plus)	❌ **NOT SAFE**	Prompts and uploaded data may be reviewed by human trainers and are used to train the general model. **Waiver of Privilege Risk.**	**PROHIBITED** for all work involving client, case, or firm confidential data.
	Gemini (Free / Advanced)	❌ **NOT SAFE**	Data may be retained, analyzed, or stored outside enterprise control. Lacks sufficient contractual data protection guarantees.	**PROHIBITED** for all work involving client, case, or firm confidential data.
	Microsoft Copilot (Bing/Free)	❌ **NOT SAFE**	User data is not confined within your organizational M365	**PROHIBITED** for all work involving

			tenant and lacks enterprise data protection policies.	client, case, or firm confidential data.
1. Consumer/Free	**Claude (Free / Pro / Max)**	❌ **NOT SAFE**	Default settings often require the user to *opt-out* of training and data retention can still be up to 30 days or longer for flagged content.	**PROHIBITED** for all work involving client, case, or firm confidential data.
2. Business/Team	ChatGPT (Team $25–30/mo)	**✓ SAFER, BUT LIMITED**	Prompts are generally not used for training, offering a layer of privacy. **Lacks the dedicated compliance controls of Enterprise.**	**USE WITH EXTREME CAUTION.** Requires firm-wide policy to strip all PII/confidential details before use. Best limited to internal-only, non-client tasks.
	Gemini (Workspace $20–30/mo)	**✓ SAFER, BUT LIMITED**	Workspace accounts provide better admin control, but contractually may not meet the highest legal compliance standards (e.g., HIPAA-ready).	**USE WITH EXTREME CAUTION.** Requires firm-wide policy to strip all PII/confidential details before use. Best limited to internal-only, non-client tasks.
	M365 Copilot (Business)	**✓ SAFER, BUT LIMITED**	Data is confined within the M365 tenant boundary. Requires specific M365 Business licenses	**USE WITH EXTREME CAUTION.** Requires legal compliance sign-off. Still needs human oversight to

			(e.g., Standard/Premium).	prevent "hallucinations."
2. Business/Team	**Claude for Work / API (Standard)**	**✓ SAFER, BUT LIMITED**	API data is generally **not** used for model training by default, offering strong data controls. Web UI version typically retains data for 30 days.	**USE WITH EXTREME CAUTION.** Use strictly via commercial API key, not the web interface, and ensure ZDR is contracted.
3. Enterprise	**ChatGPT Enterprise** (Custom $60+/mo)	**✓✓ MANDATORY TIER**	SOC 2 certified, private instance, and includes **contract-based Zero Data Retention (ZDR)** clauses prohibiting use of prompts for model training.	**RECOMMENDED** for professional integration. Must confirm ZDR is active and enforced.
	Gemini Enterprise ($30+/mo)	**✓✓ MANDATORY TIER**	Compliance-grade controls, dedicated admin, and robust ZDR guarantees.	**RECOMMENDED** for professional integration. Must confirm ZDR is active and enforced.
	Microsoft Copilot (M365 E3/E5 + Copilot $30+/mo)	**✓✓ MANDATORY TIER**	Protected via the **Microsoft Purview** security framework. HIPAA-ready and confines data within the organizational tenant.	**RECOMMENDED** for professional integration, especially for firms already using the Microsoft ecosystem.
3. Enterprise	**Claude API (ZDR Addendum)**	**✓✓ MANDATORY TIER**	Optional **Zero Data Retention (ZDR) addendum** provides the maximum level of	**RECOMMENDED** for professional integration. Requires a signed

		data isolation and deletion (0 days retention).	ZDR contract addendum for guaranteed 0-day retention.

II. Ethical Pillars for Responsible AI Use

Adopting an Enterprise-grade solution meets the primary confidentiality requirement, but the legal professional must address these four continuing duties:

1. Duty of Competence (Model Rule 1.1)

The lawyer is **fully accountable** for the output of any AI tool, regardless of the tier used.

- **Trust But Verify:** Never assume AI output (legal citations, facts, or strategy) is correct. All GenAI outputs must be independently validated against reliable, primary sources (e.g., case law databases, statutes).
- **Understand Limitations:** You must understand the specific capabilities and known risks (like "hallucination," bias, or outdated information) of the AI model you are using.
- **Avoid Frivolous Claims (Model Rule 3.1):** Submitting AI-generated information that contains non-existent case law (a known risk) can result in professional sanctions.

2. Duty of Confidentiality (Model Rule 1.6)

Even with Enterprise protections, vigilance is required to protect the attorney-client privilege.

- **Anonymize (Best Practice):** Whenever possible, strip all personally identifiable information (PII) or unique identifying case details from prompts before submitting them, even to an Enterprise-level system.
- **Review Contractually:** The lawyer or the firm's IT department must review the Terms of Use and contractual Data Processing Addendums (DPAs) to ensure explicit, iron-clad assurances that client data is not retained or used for training.

3. Duty of Communication (Model Rule 1.4)

Transparency with the client regarding the use of technology may be required.

- **Informed Consent:** If the use of a GenAI tool involves disclosing *any* client confidential information (even to a secure enterprise system), or if it impacts the scope, expense, or strategy of the representation, the lawyer must obtain the **client's informed consent** beforehand.

- **Fees:** Lawyers cannot bill clients for time saved by using AI or for time spent learning how to use a general AI tool. Fees must always be reasonable and reflective of actual professional work performed.

4. Duty of Supervision (Model Rule 5.1 and 5.3)

The use of AI must be governed by firm-wide policies.

- **Establish Protocol:** Law firms and DR organizations must establish clear, written internal policies outlining which AI tools are approved (Tier 3 only), what data is prohibited, and the mandatory verification steps for all AI-generated work product.
- **Training:** All employees (lawyers, paralegals, mediators, and non-lawyer staff) must be trained on these policies and the risks of using consumer-grade tools.

*Prepared as a Directive for the AI Tools in Practice Workshop (2025). This document does not constitute legal advice. Consult your jurisdiction's latest Ethics Opinions.