2026 EDITION

AI Ethics Checklist for Lawyers

What Every Attorney Must Know Before Using AI in Client Work

AI is already inside your firm. The question is whether you're using it in a way that protects your clients, your license, and your practice — or one that doesn't. This checklist does not create an attorney-client relationship. It is for educational purposes only and does not constitute legal advice. Consult your state bar ethics rules and qualified ethics counsel before modifying your AI practices.

MAKO WORKFLOW · COMPLIANT AI FOR LAW FIRMS · MAKOWORKFLOW.COM

ABA RULE 1.6

Confidentiality & Data Privacy

The Rule. Rule 1.6 prohibits attorneys from disclosing information relating to the representation of a client unless the client gives informed consent or an exception applies. Rule 1.6(c) separately requires attorneys to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation. In 2026, transmitting client data to a third-party AI system implicates both provisions.

KEY AUTHORITY

- **ABA Formal Opinion 512 (2024):** Attorneys may use AI tools for client matters, but must take reasonable precautions, including confirming no-training clauses, reviewing data retention policies, and obtaining informed consent for high-sensitivity matters.
- **Rule 1.6(c) Reasonable Safeguards:** The standard is not perfection. It is whether the attorney took precautions proportionate to the sensitivity of the information and the risk of disclosure.
- **State Bar Overlay:** ABA Opinion 512 is a floor. TX Opinion 705, NY, CA, and OR have all issued guidance that imposes stricter requirements. Check your state bar before deploying any AI tool on client matters.

In Practice for Law Firms:

No-Training Clause

I have confirmed my AI vendor does not use client data to train its models, and I have a written no-training clause in our commercial agreement — not merely an opt-out setting or toggle.

Data Retention Standard

The vendor's retention period is defined and limited — not indefinite. I have confirmed attorney-controlled deletion rights and know how to exercise them. I understand that indefinite retention of client data without deletion rights does not satisfy Rule 1.6(c). Feedback buttons on any platform trigger up to 5-year retention and override deletion — do not use on client matters.

Encryption in Transit

I have confirmed my vendor uses TLS 1.2 at minimum — TLS 1.3 preferred — to protect client data from interception between my device and the vendor's servers.

Encryption at Rest

I have confirmed my vendor uses AES-256 encryption for client data stored on its servers.

No Routine Human Access (Contractual)

I have confirmed my vendor contractually restricts personnel from accessing my client data except under defined carve-outs: safety review, legal process, and customer-initiated support only. All consumer plans fail this standard. See the Privilege page for the Heppner analysis.

Written Prompt Guidelines

My firm has written guidelines specifying what information attorneys may and may not include in AI prompts and submitted documents, calibrated to each approved platform's tier and protections.

Commercial Plans Only

I use a commercial AI plan (Team, Business, Enterprise, or API) — not a consumer or individual subscription — for any work involving client documents or confidential information. Consumer plan opt-outs are settings, not contracts, and do not satisfy the standard. What matters is whether the plan provides the required contractual protections — a no-training commitment, defined retention with deletion rights, restricted human access, and SOC 2 Type II certification. Verify current terms directly; vendor plan structures and labels change.

Written Client Consent

For high-sensitivity matters, I have obtained written client consent before using AI tools to process their documents. Consent explains what tool will be used, what data will be input, and what residual risks remain, per ABA Opinion 512. Note: boilerplate engagement letter language is not sufficient — consent must be specific and informed.

ⓘ **Why it matters:** Under Rule 1.6, transmitting client information to a third-party AI system can constitute a disclosure even if no human ever reads it. Rule 1.6(c) separately requires reasonable efforts to prevent inadvertent disclosure. The question is not just whether a disclosure occurred, but whether the attorney took appropriate precautions proportionate to the sensitivity of the information. ABA Opinion 512 (2024) is clear on this.

ATTORNEY-CLIENT PRIVILEGE | WORK PRODUCT DOCTRINE

Privilege & Work Product Protection

⚠ **Critical Issue — Emerging Court Split:** Three federal courts have split on a foundational privilege/work-product question: does using a consumer AI platform constitute a disclosure that destroys confidentiality? *Heppner* says yes — the vendor's consumer terms reserve rights to retain, train on, and disclose inputs to third parties including the government, eliminating any reasonable expectation of confidentiality. *Warner* and *Morgan* say no — AI tools are instruments, not persons; waiver requires disclosure to an adversary, which doesn't occur simply by using a tool. The privilege question remains unresolved for represented parties in civil litigation. Separately, a fourth court — *Jeffries* — reached the issue through eDiscovery rather than privilege, banning public AI tools for *all* discovery materials (even non-confidential ones) by protective order and treating enterprise zero-retention terms as a court-ordered requirement. Treat all AI tool use as potentially discoverable until appellate courts provide clearer guidance.

The Rule. The attorney-client privilege protects confidential communications between attorney and client made for the purpose of obtaining legal advice. The work product doctrine separately protects materials prepared in anticipation of litigation. Both protections are at risk when AI tools are used without appropriate controls, particularly when prompts externalize mental impressions or when consumer tools log and retain inputs.

☐ **KEY AUTHORITY**

- **U.S. v. Heppner (S.D.N.Y., Feb. 2026):** In a criminal case, court denied privilege *and* work product protection for inputs submitted to a consumer Claude account. Consumer terms reserving rights to retain, train on, and disclose inputs to third parties — including government authorities — eliminated confidentiality. Work product denied because materials were not prepared at or under counsel's direction. *Commercial terms that contractually prohibit training and restrict disclosure to defined carve-outs remove the predicates the court relied on.*
- **Emerging Federal Split — Three Courts, No Consensus (2026):** Two subsequent decisions reached more protective conclusions. *Warner v. Gilbarco, Inc.* (E.D. Mich., Feb. 2026) held AI tools are instruments, not persons; a pro se plaintiff's AI-assisted litigation materials were protected work product; using an AI platform does not constitute waiver. *Morgan v. V2X Inc.* (D. Colo., Mar. 2026) also protected work product for a pro se plaintiff, rejected Heppner's confidentiality waiver reasoning, but ordered disclosure of the AI tool's identity and entered a protective order requiring enterprise-tier terms for any confidential AI input. The three privilege/work-product courts agree on the practical point: consumer tools carry higher risk; enterprise contractual terms are the emerging legal standard. The open question — unresolved for represented parties in civil litigation — is whether using a consumer AI platform constitutes a disclosure that destroys confidentiality, which affects both privilege and work product equally.
- **Jeffries v. Harcros Chemicals Inc. (D. Kan., Mar. 2026) — the furthest-reaching:** Not a privilege ruling but a discovery-management one. The court amended the protective order to ban public/open AI tools for *all* produced documents — even those not designated confidential — reasoning that data fed to public AI is practically impossible to claw back and creates a centralized repository risking data-privacy violations. This goes further than *Morgan*, which restricted AI only for Confidential Information. The upshot: a court may bar public AI from an entire matter, and enterprise AI with contractual zero-retention terms is increasingly a court-ordered requirement, not just best practice. Using a public AI tool to summarize an opponent's production could violate such an order.
- **Work Product Best Practice:** Ensure attorney direction of any AI-assisted legal work is documented, not assumed. Prompts that externalize mental impressions — e.g., "What are our weakest indemnity positions?" — may constitute opinion work product and could be discoverable if logged or disclosed by a consumer platform.

In Practice for Law Firms:

Consumer Tools Prohibited

I do not use consumer AI tools for any work involving privileged communications or litigation strategy. *Heppner* provides substantial support for the argument that consumer terms may defeat both privilege and work product protection; the *Morgan* and *Jeffries* courts' protective orders codify enterprise-tier contractual protections as the required standard — *Jeffries* barring public AI from an entire document production. Commercial terms are required.

Prompt Discipline

My prompts do not externalize mental impressions or self-assessments of risk — e.g., "What are our weakest indemnity positions?" These types of prompts may expose opinion work product if logged or disclosed.

No Routine Human Review Rights

I have confirmed my vendor does not reserve the right to routinely access or review my prompts or outputs. Commercial plans restrict human access to defined carve-outs: safety review, legal process, and customer-initiated support only.

Discoverable Logs Policy

My firm has considered whether AI-generated logs could be discoverable and has a retention policy that accounts for this risk.

Client AI Use Advisory (Rule 1.4)

Clients using consumer AI to research their legal exposure or prepare for attorney consultations may be creating discoverable, unprotected records of their legal strategy — as illustrated by *Heppner*, where a client's pre-consultation AI research lost privilege protection entirely. For litigation and sensitive matters, consider advising clients proactively about this risk. This is a Rule 1.4 communication obligation: material information the client would reasonably want to know. It does not require supervising client AI use — only informing clients of a risk they may not know exists.

Why it matters: Three federal courts divide on a foundational question that affects both privilege and work product: is using a consumer AI platform a disclosure that destroys confidentiality? *Heppner* says yes — consumer terms that reserve rights to retain, train on, and disclose inputs to the government eliminate confidentiality entirely. *Warner* and *Morgan* say no — AI is a tool, not a person; waiver requires disclosure to an adversary, not merely use of an intermediary. For represented parties in civil litigation, that question is unresolved. A fourth court, *Jeffries*, sidesteps privilege altogether — banning public AI for all discovery materials by protective order. Across all four decisions, the signal is the same: enterprise contractual terms that prohibit training and restrict third-party disclosure are the emerging legal standard, and courts are beginning to require them. The line is the terms of service — not the model, not the interface.

ABA RULE 1.1

Competence & Hallucination Risks

The Rule. Rule 1.1 requires attorneys to provide competent representation, including the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation. Comment 8 to Rule 1.1 requires attorneys to keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology. In 2026, competence includes understanding how AI tools work, where they fail, and how to supervise their output.

KEY AUTHORITY

- **Mata v. Avianca, Inc., 678 F. Supp. 3d 443 (S.D.N.Y. 2023):** Attorneys were sanctioned under Rule 11 for submitting AI-generated fabricated citations. Subsequent failures in candor reinforced that attorneys have an independent Rule 3.3 duty to correct the record when AI-generated errors are discovered post-filing. If you use the tool, you own the output and any errors in it.
- **Rule 1.1 Comment 8:** Competence in 2026 requires understanding AI tool limitations — including hallucination risk, probabilistic output, and the absence of legal reasoning — before relying on AI output in client work.

In Practice for Law Firms:

Probabilistic Output

I understand that AI tools generate text probabilistically. They can produce confident, wrong answers, including fabricated case citations and invented statutory references.

Independent Verification

I independently verify every case citation, statutory reference, and legal conclusion an AI tool produces before using it in client work. No exceptions.

Rule 11 Compliance

Before filing any AI-assisted work product, I have independently verified all factual assertions and citations to satisfy the reasonable inquiry standard.

Rule 3.3 Candor

I understand that Rule 3.3 requires candor to the tribunal. If AI-generated errors are discovered after filing, I have an affirmative obligation to correct the record promptly.

First Draft Only

I treat AI output as a first draft, not a final work product. My review protocol requires substantive attorney review before any AI-assisted work reaches a client or tribunal.

Junior Attorney Training

Junior attorneys on my team have been explicitly trained on hallucination risks and are required to independently verify AI analysis before relying on it.

Rule 8.4(c) Misconduct

I understand that knowingly submitting AI-generated false content to a client, tribunal, or opposing counsel may constitute professional misconduct under Rule 8.4(c), independent of Rule 3.3 or Rule 11.

ⓘ **Why it matters:** Mata v. Avianca, Inc. (S.D.N.Y. 2023) established that sanctions under Rule 11 and remedies under Rule 3.3 are both available when AI-generated errors reach a tribunal and the attorney fails to correct them. The competence obligation means a lawyer cannot plead ignorance of a tool's limitations — using AI output without verification is itself a professional responsibility violation, independent of whether the output turned out to be wrong.

RULES 5.1 – 5.3

Supervision & Firm Governance

The Rule. Rules 5.1 and 5.2 require partners and supervising attorneys to make reasonable efforts to ensure that all lawyers in the firm conform to the Rules of Professional Conduct. Rule 5.3 extends that obligation to nonlawyer assistants, including AI tools. In 2026, an AI tool that produces output used in client work is, for supervisory purposes, a nonlawyer whose work must be reviewed and approved by a licensed attorney before it reaches a client.

KEY AUTHORITY

- **ABA Formal Opinion 512 (2024):** Supervising attorneys are responsible for AI output used in client matters. Delegation to AI does not reduce the attorney's professional responsibility — it transfers the obligation to supervise.
- **TX Opinion 705 / NY / CA / OR:** Multiple state bars have issued guidance stricter than the ABA baseline. TX Opinion 705 specifically addresses supervision of AI tools and requires written policies governing their use.
- **Shadow AI Risk:** Staff using personal, non-enterprise AI accounts for firm work creates confidentiality and privilege exposure that firm policies may not cover. This is the #1 governance failure identified in 2025–26 bar guidance.

In Practice for Law Firms:

Written AI Policy

My firm has a written AI usage policy that specifies approved tools, permitted use cases, and required review steps before client delivery.

Licensed Attorney Sign-Off

A licensed attorney must review and sign off on all AI output before client delivery. High-risk outputs — litigation strategy, regulatory analysis, client advice, contract redlines — require senior attorney sign-off specifically.

Anti-Shadow AI Protocol

I have verified that staff are not using personal, non-enterprise AI accounts for any firm-related tasks. Shadow AI is the #1 governance failure in 2025–26.

Client Communication & Scope (Rules 1.2 / 1.4)

I have considered my obligations under Rules 1.2 and 1.4. Rule 1.2 requires lawyers to consult with clients on the means of representation — for AI-assisted work, this may require client input on which tools are used and how. Rule 1.4 requires ongoing communication about material developments in the representation. Clients may have a right to know AI was used in their matter, independent of consent under Rule 1.6. Best practice: address AI tool use explicitly in the engagement letter.

Agentic AI Protocol

If my firm uses agentic AI tools that take autonomous actions — drafting communications, accessing databases, filing documents — I have a specific supervision protocol for those outputs before they take effect.

Vendor Ethics Diligence

I have conducted reasonable diligence to ensure the AI vendor's internal security and ethics protocols are compatible with my professional obligations under Rule 5.3.

AI Literacy Training

All staff who interact with AI tools have received training covering hallucination risks, prompt hygiene, privilege exposure, and the prohibition on personal AI accounts for firm work — consistent with emerging 2026 state bar competence expectations.

⚠ **Why it matters:** AI tools must be supervised like any nonlawyer assistant. The more substantive the output, the heavier the supervisory obligation. In 2026, the #1 governance failure is staff using personal AI accounts for firm work — shadow AI creates confidentiality and privilege exposure your policy may not cover. ABA Opinion 512 sets the baseline; TX Opinion 705, NY, CA, and OR have all issued stricter requirements.

ABA RULE 1.5 | RULE 1.6(C) SAFEGUARDS

Billing Transparency & Vendor Due Diligence

☐ KEY AUTHORITY

- **Virginia LEO 1901 (eff. Nov. 2025):** AI efficiency gains do not per se require reduced fees. All fees must remain reasonable under Rule 1.5 factors. Document your billing methodology.
- **ABA Formal Opinion 512 (2024):** Rule 1.6(c) requires evaluating the vendor's terms — training use, retention, access, and disclosure — and implementing safeguards proportionate to the sensitivity of the information, before client data touches the vendor's system.
- **EU AI Act (2026 Enforcement):** GPAI compliance obligations are now in effect. Attorneys with EU client exposure must assess whether their vendor qualifies as a high-risk AI system and what deployer obligations that triggers for the firm.

Billing Transparency: ABA Rule 1.5

- My billing practices reflect actual time. Virginia LEO 1901 (eff. Nov. 2025) requires only that fees remain reasonable under Rule 1.5 factors regardless of structure.
- My engagement letters address AI tool use and clarify how related costs, if any, are handled.
- If a client asks whether AI was used in their matter, I can answer honestly and describe how the output was supervised.
- I do not pass through AI tool costs as disbursements without prior disclosure to the client.

Vendor Due Diligence: Rule 1.6(c)

- My vendor has **SOC 2 Type II** certification — *required*, not merely preferred. SOC 2 Type II is an independent audit of control effectiveness over time. Demand the audit report, not a marketing summary or self-reported claim.
- My vendor uses **AES-256 encryption at rest** and **TLS 1.2 minimum (TLS 1.3 preferred) in transit**, and has a documented breach-notification process with defined timelines.
- I do not click **thumbs-up/down feedback buttons** on any conversation containing client data on any platform, regardless of plan tier. Feedback triggers retention of up to 5 years, overriding standard retention periods and any deletion performed.
- The vendor's data retention period is **defined and limited**. I have confirmed attorney-controlled deletion rights. Indefinite retention without deletion controls does not satisfy Rule 1.6(c).
- The vendor's commercial terms include a **Data Processing Addendum (DPA)** covering permitted processing, subprocessors, and deletion obligations — I have located it and retained a copy. *(A GDPR-executed DPA is required if EU personal data is processed; a BAA if HIPAA data.)*

- **If my firm handles EU client or personal data:** I have confirmed where my vendor processes and stores data geographically and whether cross-border transfer restrictions (GDPR) apply — both major vendors' DPAs include Standard Contractual Clauses as the transfer mechanism.
- If my firm handles EU client data, I have assessed **EU AI Act / GPAI** compliance obligations, including whether the vendor has signed the EU AI Act Code of Practice for GPAI models with systemic risk. *(Required if EU exposure exists.)*
- I have reviewed the vendor's **trust center or security whitepaper** — not just the marketing page.

> ⚠ **Why it matters:** Rule 1.6(c) reasonable safeguards in 2026 means more than certifications alone. It means contractual protections that hold up under scrutiny, proportionate to the sensitivity of the matter — plus EU-specific obligations (GDPR transfers, GPAI) where EU exposure exists. SOC 2 Type II is required — demand the report. A vendor's promise is not a safeguard.

Quick-Reference Summary

Before using any AI tool on a client matter, can you answer the following questions?

QUESTION TO ASK YOURSELF	2026 STANDARD
Is this a commercial AI plan with a written no-training clause?	**Standard / Presumptive***
Have I confirmed the vendor restricts human access and third-party disclosure?	**Required: contractual carve-outs only**
Have I confirmed TLS 1.2+ encryption in transit and AES-256 at rest?	**Required: check trust center documentation**
Is the vendor's retention period defined, with attorney deletion rights confirmed?	**Required: defined period + deletion rights; no indefinite retention**
Have I avoided feedback buttons on this conversation?	**Required: no feedback buttons on client matters, any tier**
Has a licensed attorney reviewed this output?	**Required before client use**
Does my firm's AI policy approve this use case and govern what I may include in prompts?	**Confirm before proceeding**
Am I billing actual time and documenting my AI methodology?	**Yes: document your approach**
Have I verified all citations and legal conclusions?	**Every time, no exceptions**
Have I checked my state bar's AI ethics guidance?	**ABA Opinion 512 is a floor only**
Have I assessed EU AI Act / GPAI compliance obligations?	**Required if EU exposure exists**

QUESTION TO ASK YOURSELF	2026 STANDARD
Has staff been warned against using personal AI accounts?	**Anti-shadow AI protocol required**
Have I obtained attorney review for all client-facing outputs, senior review for high-risk ones?	**Required: attorney for all, senior for high-risk**
Do I have a SOC 2 Type II certified vendor?	**Required: demand the audit report, not a summary**

**Unless explicit informed written client consent for the use of a consumer-tier tool has been obtained for that matter.*

The bottom line: AI doesn't lower your professional obligations. It raises the stakes for meeting them. Every output you rely on is your responsibility. The tool assists. The attorney is accountable.

About Our AI Implementation Practice

We help law firms deploy AI tools that conform to the latest ethical and confidentiality standards. We are not selling a product. We are building compliant AI infrastructure for law practices.

Every implementation we deliver is designed to support compliance with ABA ethics guidance, including ABA Formal Opinion 512 (2024). Our governance framework is mapped to the NIST AI Risk Management Framework (v1.0/v2.0).

We built this practice because lawyers needed AI implementation that takes professional responsibility as seriously as speed — ensuring every deployment helps you move faster without compromising the obligations you've built your practice on.

ABA Formal Opinion 512 (2024)	**Mapped to NIST AI RMF (v1.0/v2.0)**
SOC 2 Type II Framework	**Heppner-Aware Architecture**

Our Credentials

- Built by lawyers, for lawyers
- Designed to support compliance with ABA Formal Opinion 512 (2024) & Model Rules 1.1, 1.2, 1.4, 1.6, 5.1–5.3
- Enterprise-grade privacy by design: no-training clauses, AES-256 encryption at rest, TLS 1.3 in transit, and tenant isolation. Ask for our data handling summary.
- Governance mapped to the NIST AI Risk Management Framework — the framework that holds up under bar scrutiny

Red Flags That Require Immediate Action

If any of the following apply to your firm, address them before using AI on another client matter. Each represents a documented compliance gap under current bar guidance.

Staff Using Consumer AI on Client Work

Any attorney or staff member using ChatGPT Free, Claude Free, or any consumer-tier AI for client matters without specific written client consent. Consumer opt-outs are revocable settings, not contracts — they do not satisfy Rule 1.6(c)'s reasonable safeguards requirement. This is the most common compliance gap in the profession today.

No Written AI Policy

Your firm has no written policy specifying approved AI tools, permitted use cases, prohibited inputs, and required review steps before client delivery. Rules 5.1 and 5.3 require this. A policy that exists on paper but has not been communicated to staff does not satisfy the supervisory obligation.

No AI Tool Inventory

You cannot identify every AI tool currently in use at your firm. Shadow AI — personal accounts used for firm work — creates confidentiality and privilege exposure your policy may not cover. The #1 governance failure identified in 2025–26 bar guidance.

No Attorney Review Requirement

AI outputs reach clients without a licensed attorney reviewing and approving them. Rule 1.1 requires independent verification of every AI output used in client work. No exceptions. The tool assists; the attorney is accountable.

No Commercial Terms for Client Work

AI tools used for client matters operate under consumer terms rather than commercial contracts. What matters is whether the plan provides a contractual no-training commitment, defined retention with deletion rights, restricted human access, and SOC 2 Type II certification — not the plan's label. Verify current terms directly.

No Retention Practice Established

You have not confirmed your vendor's data retention period, do not know how to delete conversations, and have no practice for deleting client-matter conversations at matter close. Indefinite retention of client data without deletion controls does not satisfy Rule 1.6(c). Note: feedback buttons on any platform override any deletion performed and trigger up to 5-year retention.

No SOC 2 Type II Verification

You have not requested or reviewed your vendor's SOC 2 Type II audit report. A vendor's self-reported security claims are not independent verification. Type II confirms controls operated effectively over time — Type I does not. Demand the audit report; both Anthropic and OpenAI provide it to commercial customers under NDA through their trust centers.

No Client Advisory on AI Use Risks

For litigation or sensitive matters, you have not advised clients about the risk of using consumer AI to prepare for attorney consultations. *Heppner* illustrates that client-generated AI materials can lose privilege protection before the first attorney meeting. Under Rule 1.4, clients should be informed of material risks they may not know exist.

If you checked 3 or more boxes: Your firm should conduct an AI governance review before expanding AI use on client matters. These gaps create professional responsibility exposure that accumulates with each matter where they go unaddressed.

Where Does Your Firm Stand?

If any red flag on the previous page applies to your firm — or you can't say for certain that it doesn't — that's worth twenty minutes. On our free 20-minute Time-Leak Check we'll talk through the flags that concern you and where your firm's hours are going. If a deeper look is warranted, our Workflow Assessment includes a verified governance readiness review alongside fixed-price automation proposals. No sales pressure.

01 — Talk Through Your Flags

Which of the red flags apply to your firm, and which ones create the most exposure today.

02 — See Where the Hours Go

A first pass at where your firm's time is leaking — the workflows that leak time are usually where the governance gaps live.

03 — Know Your Next Step

Leave with your highest-priority gaps, the right questions for your ethics counsel, and an honest answer on whether a full Workflow Assessment is worth it.

→ Book Your Free 20-Minute Time-Leak Check

Educational purposes only — not legal advice. Consult your state bar and qualified ethics counsel. · *Mako Workflow © 2026. All rights reserved.*