

AI Readiness Guide for Law Firms: Ethics, Privilege, and Client Data

How law firms can govern AI use, protect client confidences, and show clients and carriers how they do it

By AdvancedBITS | Business IT Solutions • Updated October 21, 2026 • About 15 minutes to read

Quick answer: what is AI readiness for a law firm?

AI readiness for a law firm means knowing which AI tools lawyers and staff actually use, confirming what each tool does with client information, keeping a named attorney responsible for reviewing AI-assisted work, protecting access with strong security and tested backups, and being able to show a client or carrier how the firm does all of that. This guide gives you a tool-terms checklist, a 12-question scorecard, a one-page client AI statement template, and a 90-day plan.

Lawyers are adopting AI faster than firms are governing it, while the duties of confidentiality, competence, supervision, and candor have not changed. Clients, carriers, and courts are starting to ask how firms handle the gap. For a five-minute version, read our [executive overview](#).

General information about technology risk, not legal advice. Your ethics counsel decides what your jurisdiction's rules require. Statistics are linked to their sources, and the research table says how strong each source is.

What does the research say about AI in law firms?

Short answer: individual lawyers are adopting AI faster than their firms govern it, while clients, courts, and attackers are already paying attention.

Finding	Source	Why it matters
69% of legal professionals use general-purpose generative AI for work, up from 31% a year earlier. Only 46% of firms have implemented those tools at the firm level, 54% offer no AI training, and 43% have no AI governance policy (1,300 respondents).	8am 2026 Legal Industry Report . Vendor-run survey.	Individual use is ahead of firm governance.
The biggest barriers to adoption are data security (46%), ethical issues (42%), privilege concerns (39%), and lack of trust in results (39%). 52% of firms choose AI tools built into their existing practice management software, and firm use of legal-specific AI tools rose from 21% to 34%.	8am summary ; ABA Law Practice Magazine . Vendor-run survey.	Lawyers already name the right worries, and embedded AI belongs on the inventory.
38% of surveyed legal professionals save 1 to 5 hours a week with AI, and 14% save 6 to 10 hours.	ABA Law Practice Magazine . Self-reported.	This is the upside that governance protects.
2,202 court decisions (as of October 19, 2026) in which a court found or implied that a party relied on hallucinated content, involving lawyers and self-represented litigants. The database also includes a few decisions where AI use was alleged but not confirmed.	Charlotin AI Hallucination Cases Database . Public database, updated often.	Verification has to be provable, not just promised.
Of 657 in-house legal professionals, 59% were not aware whether their law firms use generative AI, and 61% plan to push for changes in how legal services are delivered and priced.	ACC/Everlaw survey ; press release . 2025 survey, run by ACC and a vendor.	Clients will ask, and many are not sure what their firms do.
85% of in-house legal departments now deploy AI, up from 53% a year earlier (576 in-house professionals surveyed in July 2026).	ACC 2026 survey report . Public summary. The full report is members-only.	Your clients' questions will be informed.

Finding	Source	Why it matters
BakerHostetler handled more than 1,250 incidents in 2025. Its report says employees pasting company data into unapproved generative AI tools is “more common than you think,” and 25% of the incidents it handled occurred at a vendor.	BakerHostetler 2026 report . Primary.	Shadow AI and vendor risk show up in real incident data.
The FBI says the Silent Ransom Group has targeted U.S. law firms since spring 2023. Callers pose as the firm’s IT support, some impersonators visit in person, data is stolen without encrypting anything, and victims and their clients are pressured.	FBI notice, May 2025 ; FBI alert, May 2026 . Primary.	Law firms are a named target, so security basics are part of AI readiness.
Underwriters are focused on AI oversight, training, and supervision, affirmative AI coverage typically depends on documented governance, and only one of the printed malpractice applications that source reviewed asked about AI. One major carrier says it is not asking supplemental AI questions.	Legal AI Governance guide ; The Redline . Secondary, and practices vary.	Know your answers before the renewal form arrives.
Multifactor authentication reduced the risk of account compromise by 99.22% across the population studied.	Microsoft Research, May 2023 . Primary.	Identity controls protect every account AI tools use.
Phish-prone percentage fell 87% after 12 months of continuous training and testing, from 33.2% to 4.2%. This is a global, cross-industry average.	KnowBe4, 2026 report . Vendor benchmark.	Training works over months, not weeks.
69% of small and mid-sized businesses refused ransom demands because they had reliable backups.	Cyber Readiness Institute, summarizing Verizon’s 2026 report . Secondary.	Tested backups give you a choice.

Where does AI show up inside a law firm?

Short answer: personal accounts, extensions, meeting bots, AI inside licensed tools, and Copilot.

Shadow AI is the use of AI tools, accounts, extensions, or meeting bots that the firm has not reviewed or approved. Most firms look for AI in the tools they bought on purpose, but it also arrives through the side door. A complete inventory covers all five places below.

Where	What it looks like	Why it matters to a firm
Personal chatbot accounts	Lawyers or staff use ChatGPT, Gemini, Claude, or Perplexity through personal logins.	The firm cannot see the terms, retention, or training use, and cannot manage the account. The privilege ruling discussed below involved a consumer tool.
Browser extensions and writing assistants	Add-ons that summarize pages, rewrite emails, or read documents open in the browser.	They can request broad access to what is on screen, including client documents.
Meeting and transcription bots	Note-takers that join calls, record, and produce summaries.	Privileged discussions may be recorded and stored outside the firm’s systems.
AI inside tools the firm already licenses	New AI features in practice management, document management, research, e-discovery, and productivity software, sometimes on by default.	Approved years ago, before the AI features existed. Each one needs the same terms review as a new tool.
Microsoft 365 Copilot and similar assistants	Assistants that answer using mail, files, and chats. Microsoft says Copilot uses data a user can already access.	A gap in a permissions-based ethical wall matters more once the assistant is on.

Also inventory **remote-access software**. It is not AI, but the FBI alerts describe attackers using legitimate remote-access tools to get into law firms. For the controls behind this inventory, see the [Legal AI Operating Model for Law Firms](#).

What does ethics guidance say about lawyers using AI?

Short answer: lawyers may use generative AI, but the existing duties of competence, confidentiality, communication, supervision, candor, and fees all apply.

The guidance below is advisory, so check your own state bar’s rules. The right-hand column is our checklist of what a firm should be able to show, not a statement of what any rule requires.

Duty	What the guidance says	What a firm should be able to show
Competence	ABA Formal Opinion 512 says lawyers should understand the benefits and risks of the technologies they use. Texas Opinion 705 points to technological competence, especially in preserving client confidential information.	Training records and an approved-tool list that notes each tool’s limits.
Confidentiality	Opinion 512: keep all information relating to the representation confidential unless the client gives informed consent. Florida Opinion 24-1 : research a tool’s policies on data retention, data sharing, and self-learning.	A terms review for every tool that touches client information (checklist in the next section).
Communication	Opinion 512 points to the duty to reasonably consult with the client about the means used to accomplish the client’s objectives.	A client-facing AI statement and engagement-letter language your ethics counsel has reviewed.
Supervision and candor	Opinion 512 lists supervising employees and agents and candor toward the tribunal among the duties that apply. Florida 24-1 says lawyers must develop policies and practices to verify that AI use is consistent with their obligations.	A named reviewer for AI-assisted work, and a record of who verified citations and quotations on each filing.
Fees	Opinion 512 says a lawyer may charge for time spent entering information into an AI tool and reviewing the output, but in most circumstances cannot charge a client for learning how to use the tool.	Billing guidance for AI-assisted work that matches your fee agreements.

Does using AI put privilege at risk?

Short answer: not automatically. One court found a defendant’s use of a consumer AI tool unprotected, and commentators disagree on how far that ruling reaches.

In *United States v. Heppner* (S.D.N.Y., February 2026), a criminal defendant who had received a grand jury subpoena and retained counsel used the consumer version of an AI tool on his own initiative, without his lawyers’ direction, to prepare defense-strategy reports, then shared them with his lawyers. Judge Rakoff held the documents were protected by neither attorney-client privilege nor work product. [Debevoise’s analysis](#) gives his reasons, including that the AI is not a lawyer and that the consumer tool’s privacy policy let the provider disclose user data to third parties, so there was no reasonable expectation of confidentiality.

[Venable](#) says the court applied traditional, technology-neutral privilege principles, and that attorney-directed use under enforceable confidentiality frameworks “may present a materially different analysis.” A [Harvard Law Review essay](#) argues the opinion as written “veers toward categorically excluding” a client’s use of generative AI from privilege. A [Legal IT Insider report](#) quotes a former S.D.N.Y. judge, Katherine Forrest, calling the ruling narrower than its reputation, and notes it is not settled: an E.D. Michigan magistrate judge reached the opposite conclusion on work product the same day.

The practical takeaway is ours, not the court’s: keep client use of public AI tools out of privileged matters unless counsel says otherwise, and put attorney-directed use on firm-managed accounts with reviewed terms. Ask counsel how the ruling applies to you.

How do you review an AI tool's data terms before using it on client work?

Short answer: find out whether the account is firm-managed, whether the provider trains on your inputs, how long data is kept, who can receive it, and whether you can see who used the tool.

Run this checklist on every AI tool that could touch client information. The questions follow [Florida Opinion 24-1](#) and the terms issues in *Heppner*. Terms differ by plan, so check the plan you hold. A “no” or “not sure” on any row is a reason to pause that tool for client work until it is resolved.

#	Ask	Why it matters	Our answer and notes
1	Is this a personal or consumer account, or a business account the firm administers?	The consumer tool in Heppner is the cautionary example, and the firm cannot manage or audit a personal login.	
2	Does the provider train its models on our inputs and outputs?	Florida 24-1 tells lawyers to research self-learning. Client information should not become training data.	
3	How long are prompts, files, and outputs kept, and can we delete them?	Florida 24-1 names data retention. Unlimited retention extends the exposure window.	
4	Who can the provider disclose our data to, and in what circumstances?	Disclosure language in a privacy policy undercut the privilege claim in Heppner.	
5	Which other companies and locations handle the data?	Vendor-side incidents appear in real incident data (see the research table).	
6	Does the contract include confidentiality commitments, security standards, and notice to us if there is a breach?	You carry the duty to the client, so the contract should support it.	
7	Can we see who used the tool and what was uploaded?	You cannot supervise or answer a client's question without logs.	
8	Does the tool respect our permissions and ethical walls, or does it index everything?	Microsoft says Copilot uses data a user can already access.	
9	Do any client guidelines or engagement letters restrict this tool or require disclosure or consent?	ACC publishes sample outside counsel AI guidelines that cover disclosure, data security, accuracy, and performance.	
10	What happens to our data if we stop using the tool?	You need export and deletion rights before client data goes in.	

How ready is your law firm for AI? The AI Readiness Scorecard

Short answer: twelve questions across six areas, scored 0 to 24.

AI governance for a law firm is the set of rules, controls, and records that show which AI tools are approved, how client information is protected, and who reviews AI-assisted work. Score each question 2 for Yes, 1 for Partly, 0 for No. The AdvancedBITS AI Readiness Scorecard and its bands are an illustrative self-assessment, not an audit, a published benchmark, or a compliance determination.

#	Area	Question	Yes (2)	Partly (1)	No (0)
1	Governance and policy	We have a written AI acceptable-use policy that names approved, restricted, and prohibited tools and data, reviewed in the last 12 months.			
2	Governance and policy	We check client outside counsel guidelines and engagement letters for AI restrictions, and handle disclosure or consent where they require it.			

#	Area	Question	Yes (2)	Partly (1)	No (0)
3	Data and permissions	We have reviewed the data terms of every AI tool that touches client information, using a checklist like the one above.			
4	Data and permissions	We test matter permissions and ethical walls in Microsoft 365 before turning on an AI assistant such as Copilot.			
5	Identity and security	Multifactor authentication is on for every user and every system that holds client information.			
6	Identity and security	Staff are trained to verify unexpected IT-support calls, and IT staff follow a procedure for authenticating themselves to employees.			
7	Resilience and recovery	Our backups cover Microsoft 365 data, and we have actually tested a restore.			
8	Resilience and recovery	Our incident plan covers client data pasted into an unapproved AI tool and a data-theft extortion attempt.			
9	People and review	A named attorney must review AI-assisted work before it goes to a client or a court.			
10	People and review	We keep a record of who verified citations and quotations on each filing, and we train lawyers and staff by role.			
11	Measurement	We have a current inventory of the AI tools in use, including personal accounts, extensions, and meeting bots, and we review it at least quarterly.			
12	Measurement	We could give a client's general counsel a documented account of how we govern AI within a day.			

- **20 to 24:** a solid foundation. Document it, test it, and schedule the quarterly review.
- **12 to 19:** real gaps. Close the lowest-scoring area first, usually visibility (Q11) or tool terms (Q3).
- **0 to 11:** governance is mostly informal. Start with visibility: find out what is running before writing more policy.

What should a law firm tell clients about AI? A one-page statement template

Short answer: say plainly which tools you use and who reviews the work.

Many clients do not know what their firms do. Edit the bracketed items. Keep a sentence only if it is true for your firm today and have your ethics counsel review the final version.

How [Firm Name] Uses AI and Protects Your Information

Our approach. We may use AI tools to help our lawyers work more efficiently. We use them only in ways that keep your information confidential and keep a lawyer responsible for the work.

Which tools. We use [list approved tools] under business accounts that the firm manages. We do not enter client information into personal or consumer AI accounts.

Attorney review. A [lawyer or named role] reviews AI-assisted work before it goes to you or to a court, including checking citations and quotations against the source.

Protecting your information. Access to your matter is limited to the people working on it. We use [multifactor authentication], [tested backups], and [permission controls that enforce ethical walls].

Your choices. If you have guidelines for how we use AI on your matters or would prefer that we not use AI on your matter, please tell [contact name] and we will [follow your guidelines or discuss options with you].

Your own use of AI. Please talk with us before you enter information about your matter into a public AI tool. Depending on the tool's terms, it may not be protected by privilege. [Counsel to review this sentence.]

Billing. We bill for time spent, including time to review AI-assisted work. We do not bill you for time spent learning a tool. [Confirm against your fee agreements.]

Questions. [Name, title, email, phone]

Template for illustration. Not legal advice. Do not publish a statement you cannot back up. The scorecard above shows which statements you can support today.

What does a 90-day AI readiness plan for a law firm look like?

Short answer: a law firm can build a documented AI readiness foundation in about 90 days by discovering what is running, deciding and protecting, then documenting and reviewing.

Days	Focus	Result
1 to 30: Discover	Inventory AI tools in use, including personal accounts, extensions, meeting bots, embedded AI, and remote-access software. Run the tool-terms checklist on each. Check client guidelines. Test ethical walls and permissions.	A real picture of what is running and what each tool does with client data.
31 to 60: Decide and protect	Approve a short list of tools on managed accounts. Fix permission gaps. Confirm multifactor authentication everywhere and set the IT-verification procedure. Publish the policy and train by role.	Approved tools lawyers will actually use, and the security basics in place.
61 to 90: Document and review	Name the reviewing attorney and start the verification record. Test a backup restore. Add AI and extortion scenarios to the incident plan. Finalize the client statement. Schedule a quarterly review.	A documented account you can show a client, a carrier, or a court.

The plan is an AdvancedBITS framework, not a published standard.

Frequently asked questions about AI readiness for law firms

What is AI readiness for a law firm?

AI readiness for a law firm means knowing which AI tools lawyers and staff use, confirming what each tool does with client information, and keeping a named attorney responsible for reviewing AI-assisted work. It also means protecting access with strong security and tested backups, and being able to show a client or carrier how the firm does all of that.

Can lawyers ethically use generative AI?

Yes, if they keep their existing duties intact. [ABA Formal Opinion 512](#) and [Florida Opinion 24-1](#) both treat generative AI as usable, provided the lawyer protects client confidentiality, stays competent, supervises the work, and bills properly. ABA opinions are guidance, and your state bar's rules govern, so check your jurisdiction.

What did ABA Formal Opinion 512 say about lawyers using AI?

[ABA Formal Opinion 512](#), issued July 29, 2024, is the American Bar Association's first formal ethics opinion on lawyers' use of generative AI. It says the duties of competence, confidentiality, communication, and reasonable fees apply, and that client information stays confidential unless the client gives informed consent. The [opinion text](#) also lists supervision and candor toward the tribunal among the duties that apply.

Is it safe for lawyers to use ChatGPT with client information?

It depends on the account and its terms, not the brand. A firm-managed business account with reviewed terms is a different situation from a personal login. [Florida Opinion 24-1](#) tells lawyers to research a tool's policies on data retention, data sharing, and self-learning first, and the consumer tool in the [Heppner ruling](#) was undercut by its own privacy policy. Run the tool-terms checklist before any client information goes in, and ask your ethics counsel.

Does using AI waive attorney-client privilege?

Not automatically. The court in *Heppner* did not hold that using AI waives privilege. It held that documents a defendant created with a consumer AI tool, on his own and without his lawyers' direction, were not privileged, partly because the tool's privacy policy allowed disclosure to third parties. Commentators disagree on how far the ruling reaches, and it is one district-court decision. Review each tool's terms, use firm-managed accounts for attorney-directed work, and ask your counsel how the ruling applies.

What is shadow AI in a law firm?

Shadow AI in a law firm is the use of AI tools, accounts, extensions, or meeting bots that the firm has not reviewed or approved, often a lawyer's personal chatbot account. The firm cannot see what client information is entered or what the provider does with it, which creates confidentiality and privilege risk.

How do you vet an AI tool for law firm use?

Check five things before any client information goes in: whether the account is firm-managed or personal, whether the provider trains on your inputs, how long data is kept and whether you can delete it, who the provider can disclose it to, and whether you can see who used the tool. [Florida Opinion 24-1](#) names retention, sharing, and self-learning as the policies to research. A full review also covers contract confidentiality terms, breach notice, vendors, and exit rights.

What should a law firm AI policy include?

A law firm AI policy should name approved, restricted, and prohibited tools, say which client data may never go into unapproved tools, and require a named attorney to review AI-assisted work. It should also set up a record of citation verification, a way to request new tools, training by role, incident reporting, and an owner for AI governance.

Do law firms have to tell clients they use AI?

It depends on the tool, the data, the jurisdiction, and the client's guidelines. [ABA Formal Opinion 512](#) says client information must stay confidential unless the client gives informed consent, and points to the duty to consult with the client about the means used. [ACC publishes sample outside counsel AI guidelines](#) that cover disclosure, so a client may require it. Check each client's guidelines and ask your ethics counsel.

What happens when a lawyer files AI-generated fake citations?

Courts have sanctioned lawyers for AI hallucinations, which are fabricated AI outputs such as fake case citations. The IRS Office of Professional Responsibility's [June 2026 alert](#) summarizes the sanctions: financial penalties, often several thousand dollars, public censure, required ethics courses, default judgments, removal from the matter, and disciplinary referrals. One trade publication reports that [malpractice policies generally do not pay court sanctions](#). A record of who verified each citation is the practical defense.

What is an ethical wall, and can Copilot break one?

An ethical wall is a set of controls that keeps information about one matter away from the lawyers and staff who should not see it, usually to manage a conflict of interest. [Microsoft says](#) Copilot uses data a user can already access, so a wall built on permissions is only as strong as those permissions. Test and fix matter permissions before enabling Copilot.

How long does it take to get a law firm ready for AI?

AdvancedBITS suggests a 90-day first cycle: discover what is running and review tool terms in days 1 to 30, approve tools and close security gaps in days 31 to 60, then document, test, and review in days 61 to 90. It is a planning framework, not a published standard, and the right pace depends on firm size and current controls.

How does AdvancedBITS help law firms with AI readiness?

AdvancedBITS provides the technology foundation: visibility, security, permissions, recovery, and documentation. We do not give legal advice, and your counsel decides what your rules require.

Area	AdvancedBITS support
AI visibility	A Complimentary AI Visibility Scan: a documented picture of which AI tools and remote-access software are running, by which users, on which devices.
Tool review and policy	Help running the terms checklist, approving tools, and drafting acceptable-use guidance for your counsel to review.
Microsoft 365 permissions	Review of matter permissions and ethical walls before an AI assistant is enabled.
Identity and security	Multifactor authentication, email security, awareness training, and monitoring.
Backup and recovery	Microsoft 365 backup, restore planning, and tested recovery.
Incident readiness	Incident planning and tabletop exercises that include AI data exposure and data-theft extortion.

Start with a fifteen-minute conversation

Tell us where your scorecard landed and we will show you what is running in your firm. No cost, no obligation.

Email sales@advancedbits.com | Call 561-300-3015

AdvancedBITS | Business IT Solutions

Secure. Compliant. Outcome-Focused.

sales@advancedbits.com | www.advancedbits.com | 561-300-3015

Sources and further reading

Read survey figures as directional: several are vendor-run or self-reported, the Verizon figure and the carrier items are secondary, and the checklist, scorecard, bands, 90-day plan, and client statement are illustrative AdvancedBITS frameworks.

- Ethics guidance: [ABA Formal Opinion 512 news release](#); [Opinion 512 text](#); [Florida Opinion 24-1](#); [Texas Opinion 705](#)
- Privilege: [Debevoise, Heppner update \(Feb. 18, 2026\)](#); [Venable \(Feb. 23, 2026\)](#); [Harvard Law Review blog \(Mar. 23, 2026\)](#); [Legal IT Insider \(Oct. 19, 2026\)](#)
- Adoption and clients: [8am 2026 Legal Industry Report](#); [ABA Law Practice Magazine](#); [ACC/Everlaw survey](#); [press release](#); [ACC 2026 survey report](#); [ACC outside counsel AI guidelines \(members-only, public description cited\)](#)
- Courts and incidents: [Charlotin database](#); [BakerHostetler 2026 report](#); [BakerHostetler release](#); [IRS OPR Alert 2026-19](#)
- Threats and insurance: [FBI notice, May 2025](#); [FBI alert, May 2026](#); [SecurityWeek](#); [Legal AI Governance](#); [The Redline](#)
- Controls: [Microsoft Research MFA study](#); [KnowBe4 2026 report](#); [Cyber Readiness Institute](#); [Microsoft Learn, Copilot data foundation](#)