SBM
State Bar of Michigan

PRACTICE MANAGEMENT
RESOURCE CENTER GUIDEBOOK

QUESTIONS FOR ATTORNEYS TO ASK AI VENDORS



UPDATED: OCTOBER 29, 2026

TABLE OF CONTENTS

DATA PRIVACY, CONFIDENTIALITY, AND PRIVILEGE 3
CYBERSECURITY AND INCIDENT RESPONSE 4
ACCURACY, HALLUCINATIONS, AND LEGAL RELIABILITY 4
ATTORNEY-CLIENT PRIVILEGE, CONFLICTS, AND ETHICAL WALLS 4
OWNERSHIP, INTELLECTUAL PROPERTY,AND WORK PRODUCT 5
CONTRACT TERMS, INDEMNIFICATION, AND LIABILITY 5
AI MODELS, THIRD-PARTY PROVIDERS, AND TRANSPARENCY 6
HUMAN OVERSIGHT AND PROFESSIONAL RESPONSIBILITY 6
BILLING, PRICING, AND RETURN ON INVESTMENT 7
LEGAL WORKFLOWS AND PRACTICAL CAPABILITIES 7
AI AGENTS AND AUTONOMOUS ACTIONS 8
GOVERNANCE, COMPLIANCE, AND FUTURE READINESS 8
RED FLAGS THAT WARRANT FURTHER REVIEW 8
THE 10 QUESTIONS TO ASK IF TIME IS LIMITED 9
RECOMMENDED NEXT STEP 9
VENDOR EVALUATION SUMMARY 10

QUESTIONS FOR ATTORNEYS TO ASK AI VENDORS

Disclaimer: This checklist is for informational purposes only and is not exhaustive or legal advice. Each organization should evaluate AI vendors based on its specific needs, applicable professional obligations, and risk tolerance. Completion of this checklist does not guarantee that a vendor is secure, compliant, or suitable for legal work. Vendor representations should be independently verified and material commitments documented in writing.

When evaluating an AI vendor for a law firm, corporate legal department, or legal services organization, attorneys should focus on the following:

- confidentiality,
- attorney-client privilege,
- data security, accuracy,
- professional responsibility, and
- ownership of work product.

The goal is to determine whether the vendor's AI can be used safely with client information, whether its outputs are reliable enough for legal work, and whether the vendor's contract adequately protects the organization and its clients.

1. DATA PRIVACY, CONFIDENTIALITY, AND PRIVILEGE

These questions should be addressed before uploading client documents, pleadings, contracts, deposition transcripts, or other sensitive information.

- ☐ Will our prompts, uploaded documents, AI-generated outputs, or feedback be used to train or improve your models?
- ☐ Can you contractually guarantee that our data will not be used to train models available to other customers?
- ☐ Who can access our data, including your employees, contractors, subprocessors, and model providers?
- ☐ How do you protect information that may be subject to attorney-client privilege, the work-product doctrine, or other confidentiality obligations?
- ☐ Do you retain our data after a session ends? If so, for how long and for what purposes?
- ☐ Can we configure retention periods or require immediate deletion?
- ☐ What happens to our data when we terminate the agreement?
- ☐ Do you use customer data to generate responses for other customers, directly or indirectly?
- ☐ Where is our data stored and processed, and can we restrict processing to specified jurisdictions?
- ☐ Do you support ethical walls, matter-level access controls, and restrictions that prevent one client's information from being exposed in another client's matter?
- ☐ Will you notify us of subpoenas, court orders, or other legal demands for our data, to the extent legally permitted?
- ☐ Can you explain how using your product affects, or may affect, our obligations to preserve privilege and confidentiality?

Key follow-up: Will these commitments appear in the contract, data-processing agreement, and applicable product documentation, or are they merely statements in your marketing materials?

2. CYBERSECURITY AND INCIDENT RESPONSE

- ☐ Do you have a current SOC 2 Type II report, ISO 27001 certification, or other independent security assessment?
- ☐ Is data encrypted both in transit and at rest? How are encryption keys managed?
- ☐ Do you support single sign-on (SSO), multifactor authentication (MFA), role-based access, and audit logging?
- ☐ Can we restrict access by user, practice group, client, matter, or document?
- ☐ Do you conduct regular penetration tests, vulnerability assessments, and security reviews of AI-specific risks?
- ☐ How do you protect against prompt injection, malicious documents, data exfiltration, and unauthorized tool access?
- ☐ What is your process for identifying, investigating, containing, and reporting a security incident?
- ☐ Within what contractual period will you notify us of a suspected or confirmed breach?
- ☐ Will you provide incident reports, forensic information, and cooperation needed for client, regulator, or insurer notifications?
- ☐ What security obligations apply to your subprocessors and underlying AI model providers?
- ☐ Do you maintain cyber insurance and professional or technology errors-and-omissions coverage?

3. ACCURACY, HALLUCINATIONS, AND LEGAL RELIABILITY

- ☐ How do you test the accuracy of legal research, citations, case summaries, contract analysis, and other legal outputs?
- ☐ Has the system been independently evaluated on legal tasks relevant to our jurisdiction and practice areas?
- ☐ Can the system fabricate cases, quotations, statutory provisions, citations, or contractual language?
- ☐ Does it provide links to primary sources so that attorneys can independently verify its conclusions?
- ☐ How does it distinguish binding authority from persuasive authority, dicta, overruled cases, and subsequently amended laws?
- ☐ How current are the legal sources and databases used by the system?
- ☐ Can the system identify when it lacks sufficient information or confidence to answer?
- ☐ What safeguards prevent the system from presenting speculation as established law?
- ☐ How do you measure error rates, and will you share testing methodology and results?
- ☐ How does the system behave when sources conflict, are incomplete, or are no longer good law?
- ☐ Can we independently test the product using anonymized examples from our practice?

Practical test: Ask the vendor to demonstrate a legal research task using a known issue with controlling authority, then verify every cited case, quotation, and proposition against the original sources.

4. ATTORNEY-CLIENT PRIVILEGE, CONFLICTS, AND ETHICAL WALLS

- ☐ Do you use our data to create shared embeddings, vector indexes, memory, or other resources that could create cross-client information leakage?
- ☐ Can the platform enforce client-specific and matter-specific ethical walls?

- ☐ Can the system identify potential conflicts of interest without exposing one client's confidential information to another?
- ☐ Can we prevent AI agents from retrieving documents outside an authorized matter?
- ☐ How are shared workspaces, firm-wide search, and persistent AI memory controlled?
- ☐ Can we disable persistent memory and cross-conversation context?
- ☐ What safeguards protect confidential information when multiple attorneys use the same AI system?
- ☐ Can you explain how your architecture and contractual terms address the risk of inadvertent disclosure or waiver of privilege?

5. OWNERSHIP, INTELLECTUAL PROPERTY, AND WORK PRODUCT

- ☐ Who owns the prompts, uploaded documents, generated drafts, summaries, analyses, and other outputs?
- ☐ Do we receive a perpetual right to use, modify, reproduce, and distribute generated work product?
- ☐ Can you claim rights to our prompts, workflows, templates, legal memoranda, or proprietary legal knowledge?
- ☐ Do you use our materials to fine-tune models or create derivative products?
- ☐ What warranties or representations do you make concerning the intellectual property rights associated with your product and outputs?
- ☐ What happens if a third party alleges that an AI-generated output infringes copyright, trade secrets, or other intellectual property rights?
- ☐ Will you defend and indemnify us against qualifying intellectual property claims?
- ☐ Do you maintain records sufficient to establish the provenance of sources used in an AI-generated answer?
- ☐ Can we export all our data and outputs in usable formats when we leave the platform?
- ☐ Can you provide written confirmation of deletion, including deletion by relevant subprocessors, subject to applicable legal retention requirements?

6. CONTRACT TERMS, INDEMNIFICATION, AND LIABILITY

- ☐ Will you sign a negotiated master services agreement, confidentiality agreement, and data-processing agreement?
- ☐ Do your terms permit unilateral changes to privacy policies, model-training practices, or data retention?
- ☐ What liability caps apply to confidentiality breaches, security incidents, intellectual property infringement, and violations of data-protection obligations?
- ☐ Are confidentiality and data-security obligations excluded from your standard liability cap?
- ☐ What indemnification obligations do you accept for third-party claims, security incidents, and intellectual property infringement?
- ☐ Do you disclaim responsibility for the accuracy of your product's outputs in ways that undermine its intended legal use?
- ☐ What remedies are available if your product fails to meet contractual performance, security, or availability commitments?
- ☐ Can we terminate the agreement immediately following a material security incident, unauthorized data use, or material contractual breach?

- ☐ What happens if you discontinue the product, change the underlying model, are acquired, or become insolvent?
- ☐ Will you provide advance notice of material changes to the product, underlying models, subprocessors, or data practices?
- ☐ Can we audit compliance or obtain independent assurance reports throughout the relationship?

Negotiation priority: Review the contract's data-use provisions, security obligations, indemnities, liability caps, termination rights, and post-termination deletion requirements. A vendor's assurances are only as useful as the enforceable commitments supporting them.

7. AI MODELS, THIRD-PARTY PROVIDERS, AND TRANSPARENCY

- ☐ Which foundation models and third-party services power your product?
- ☐ Can the underlying model change without our approval or notice?
- ☐ Are our prompts and documents sent to external model providers or other subprocessors?
- ☐ Are those providers contractually prohibited from training on our data?
- ☐ Can we select the underlying model or restrict which providers process our information?
- ☐ Do you maintain a current list of subprocessors and disclose where they process data?
- ☐ How do you evaluate the security, privacy, reliability, and legal risks of model providers?
- ☐ Do you maintain documentation describing the system's intended use, known limitations, and tested capabilities?
- ☐ Can we obtain information about model versions, significant changes, and performance regressions?
- ☐ Do you offer a controlled environment, private deployment, or other architecture suitable for sensitive legal work?
- ☐ Can we disable web browsing, external integrations, plugins, and autonomous tool execution when those features are not appropriate?

8. HUMAN OVERSIGHT AND PROFESSIONAL RESPONSIBILITY

- ☐ What level of attorney review do you recommend for each supported legal use case?
- ☐ Can the product distinguish between tasks suitable for automation and those requiring professional judgment?
- ☐ Can we configure mandatory human approval before an output is sent to a client, filed with a court, or used to make a consequential decision?
- ☐ Does the platform preserve the source material and reasoning context needed for an attorney to verify an output?
- ☐ Can the system flag uncertainty, conflicting evidence, missing information, or potentially unsupported conclusions?
- ☐ Can we establish firm-wide policies that restrict certain uses of AI?
- ☐ What training do you provide for attorneys, paralegals, and administrative personnel?
- ☐ How do you notify customers when a product limitation, newly discovered risk, or material defect affects legal work?

- ☐ Can we monitor usage, investigate problematic outputs, and identify users who bypass firm policies?
- ☐ How do you support compliance with applicable state bar guidance, court rules, standing orders, and client-specific requirements?

These questions are especially important due to an attorneys ethical obligation under MRPC 1.1. Further, the ABA's Formal Opinion 512 emphasizes that lawyers retain their professional obligations when using generative AI, including duties involving competence, confidentiality, supervision, candor to tribunals, client communication, and reasonable fees.

9. BILLING, PRICING, AND RETURN ON INVESTMENT

- ☐ What is the complete cost, including licenses, usage charges, implementation, integrations, training, support, and storage?
- ☐ Are fees based on users, matters, tokens, documents, transactions, or usage volume?
- ☐ Are there hidden charges for premium models, advanced features, or additional security controls?
- ☐ Can we establish usage limits, spending caps, and alerts?
- ☐ How do you measure time savings, accuracy, quality, and return on investment?
- ☐ Can you provide independently verifiable performance data from law firms or legal departments with comparable workflows?
- ☐ How does the product affect attorney review time and the total cost of completing a legal task?
- ☐ Can we conduct a pilot before committing to a long-term agreement?
- ☐ What service levels, support response times, and uptime commitments do you guarantee?
- ☐ How should AI-assisted work be billed to clients consistent with applicable professional conduct rules and engagement terms?

10. LEGAL WORKFLOWS AND PRACTICAL CAPABILITIES

Ask the vendor to demonstrate the specific tasks your organization expects the product to perform.

- ☐ Legal research: Can the system retrieve controlling authority, verify citations, and identify negative treatment?
- ☐ Contract review: Can it identify deviations from approved clauses, missing provisions, and unusual risk allocations?
- ☐ Litigation: Can it summarize discovery, compare witness testimony, identify evidentiary gaps, and preserve source references?
- ☐ Due diligence: Can it identify inconsistencies across thousands of documents and trace each conclusion to its source?
- ☐ Drafting: Can it follow firm-approved templates, defined terms, formatting requirements, and drafting conventions?
- ☐ Regulatory compliance: Can it identify relevant requirements and provide current, authoritative source references?
- ☐ Document management: Can it retrieve the right information while respecting matter permissions and ethical walls?
- ☐ Knowledge management: Can it search internal precedents without exposing confidential information or treating outdated work product as current law?
- ☐ Integration: Does it work with our existing document management, email, practice management, research, and billing systems?

- ☐ Auditability: Can we reconstruct what documents, instructions, and model outputs informed a material legal conclusion?

For every demonstration, ask the vendor to show both a successful result and a failure case. Require the system to identify its limitations rather than simply presenting an impressive answer.

11. AI AGENTS AND AUTONOMOUS ACTIONS

If the product can do more than generate text—for example, send emails, update records, execute workflows, or interact with external systems—ask:

- ☐ What actions can the AI take without human approval?
- ☐ Can we restrict the agent to read-only access or an approved set of actions?
- ☐ Can it send client communications, change documents, submit filings, or make commitments on behalf of an attorney?
- ☐ What approval controls apply before consequential actions occur?
- ☐ Can we set transaction limits and require confirmation before external communications or irreversible changes?
- ☐ How does the system respond to malicious instructions embedded in emails, documents, websites, or retrieved content?
- ☐ Can we review an agent's activity logs and reverse actions where technically possible?
- ☐ What happens if an agent acts on inaccurate information or exceeds its authorized scope?
- ☐ Who bears responsibility for unauthorized actions, and what contractual remedies apply?

12. GOVERNANCE, COMPLIANCE, AND FUTURE READINESS

- ☐ Do you maintain a documented AI governance and risk-management program?
- ☐ How do you evaluate discriminatory outcomes, unreliable outputs, and other model risks?
- ☐ Can we obtain information about your testing methods, evaluation results, and known failure modes?
- ☐ How do you address applicable privacy laws, sector-specific requirements, records-retention obligations, and cross-border transfers?
- ☐ Can we require additional safeguards for regulated industries or particularly sensitive matters?
- ☐ How do you monitor changes in law, regulation, and court requirements that may affect the product?
- ☐ What procedures govern the release of new models and features?
- ☐ Can we test material changes in a sandbox before deployment?
- ☐ How do you maintain business continuity and disaster recovery?
- ☐ What happens to our workflows and data if the vendor changes its business model or ceases operations?

13. RED FLAGS THAT WARRANT FURTHER REVIEW

Be cautious if a vendor:

- ☐ Refuses to explain whether customer data is used for model training.

- ☐ Cannot clearly identify its subprocessors or data-retention practices.
- ☐ Relies on broad disclaimers while marketing the product as suitable for legal work.
- ☐ Cannot demonstrate reliable source citations or meaningful accuracy testing.
- ☐ Offers no adequate audit trail, access controls, or deletion process.
- ☐ Reserves unrestricted rights to change data practices or underlying models.
- ☐ Rejects reasonable security, confidentiality, or intellectual property protections.
- ☐ Cannot explain how it prevents cross-client data exposure.
- ☐ Claims that its technology eliminates the need for attorney review.
- ☐ Cannot provide meaningful documentation, security assurances, or contractual commitments.

14. THE 10 QUESTIONS TO ASK IF TIME IS LIMITED

For a first vendor meeting, prioritize these:

1. Will our client data ever be used to train or improve models, and will you contractually prohibit that use?
2. Who can access our data, where is it processed, and how long is it retained?
3. What specific controls prevent disclosure across clients, matters, and ethical walls?
4. How do you test legal accuracy, and can you demonstrate source verification?
5. What happens if the system generates fabricated authority or materially incorrect legal analysis?
6. Who owns the inputs and outputs, and what intellectual property indemnity do you provide?
7. What are your security certifications, incident notification obligations, and audit rights?
8. What liability do you accept for confidentiality breaches, data misuse, and system failures?
9. Can we require human approval, control autonomous actions, and audit material AI activity?
10. Will you put all material privacy, security, training, retention, and liability commitments in a signed agreement?

RECOMMENDED NEXT STEP

Have the vendor complete a written questionnaire, review its contractual terms, and participate in a controlled pilot using synthetic or appropriately anonymized legal materials. Before production use, involve the firm's ethics counsel, IT/security team, privacy counsel, and procurement or risk-management function as appropriate.

For the professional responsibility component, start with MRPC 1.1 and the ABA's Formal Opinion 512 on Generative Artificial Intelligence Tools , then check the rules and court-specific requirements applicable to the jurisdictions in which the attorneys practice.

VENDOR EVALUATION SUMMARY

Overall assessment

- Suitable for further consideration
- Suitable subject to additional safeguards
- Requires further legal or security review
- Not recommended for current use

Outstanding concerns:

_____
_____
_____
_____

Required follow-up documentation:

_____
_____
_____
_____

Next steps and responsible parties:

_____
_____
_____
_____

Final approval

Legal/ethics review: _____

IT/security review: _____

Procurement/risk review: _____

Approval date: _____

Note: The questions in this checklist are compiled from various articles, websites, conferences, and discussions with AI vendors. They are intended to help attorneys evaluate AI solutions and are not exhaustive. Attorneys should independently verify information and assess each vendor based on their firm's specific needs and requirements.