GenAI Tool Evaluation Checklist for Legal Practice

A Framework for State Bar of Arizona Members

Understanding AI in Legal Practice

GenAI tools present significant risks requiring systematic evaluation before use in legal practice:

Output reliability: AI can generate convincing but fabricated content including false citations, inaccurate legal analysis, and fictitious facts. Attorneys have been sanctioned for filing fabricated authorities. All AI outputs require verification appropriate to their intended use.

Data handling: Information entered into AI systems may be stored, used for model training, shared with third parties, or processed in ways that can compromise client confidentiality. Understanding a tool's data practices is essential before inputting any client information.

Professional responsibility: Your obligations under the Rules of Professional Conduct, including competence, confidentiality, supervision, and candor, apply fully to AI-assisted work. The duty of competence includes understanding the technologies you use in your practice. You bear complete responsibility for the accuracy and appropriateness of AI-assisted work product.

This checklist helps you evaluate whether a GenAI tool can be used consistent with these obligations, including your duties of competence, confidentiality, supervision, and communication under the applicable Rules of Professional Conduct.

When To Use This Checklist

Use this checklist before you:

- ☐ Adopt a new GenAI tool for use in your practice
- ☐ Allow staff or other non-lawyers to use AI on client matters
- ☐ Input any confidential, privileged, or regulated data into an AI tool
- ☐ Use AI-generated content in court filings, legal opinions, or client advice
- ☐ Renew or materially change an existing AI vendor relationship
- ☐ Reassess existing AI tool use against current standards

Part I: Firm Governance

Establish Oversight and Policy

☐ Review applicable bar ethics opinions and guidance on AI use in legal practice.

☐ Designate a person or group responsible for evaluating, approving, and overseeing AI tool use. For solo practitioners, consider support from technology advisors as needed and available; for firms, designate a partner or committee.

☐ Create and maintain a written AI policy addressing:

- Approved and prohibited tools
- Use cases requiring specific approval before use
- Requirements that must be satisfied before inputting privileged communications, work product, confidential client data, or regulated information
- Human review, verification, and approval requirements for AI-generated content
- Client notification and consent protocols
- Recordkeeping requirements

☐ Before uploading any information to a new tool, including during trial or pilot periods, ensure you understand the tool's data handling practices and have appropriate protections in place.

☐ Ensure users understand how GenAI works, its limitations, verification procedures, and applicable policy requirements through training, education, or other appropriate means

☐ Establish monitoring appropriate to your practice through periodic reviews to confirm compliance with firm policy.

Assess Your Use Case

Before evaluating specific tools, consider your intended use:

☐ Identify your use case: legal research, document drafting, contract analysis, case assessment, client communication, or other applications.

☐ Assess the sensitivity of information you may input: Will it include privileged communications, work product, confidential client information, or regulated data (such as health information or financial data)? Note: ER 1.6 confidentiality is extensive and beyond the attorney-client privilege.

☐ Evaluate your risk tolerance: What are the consequences if AI outputs contain errors? Consider potential for court sanctions, malpractice exposure, client harm, or regulatory violations.

☐ Consider whether AI is appropriate for this use case, including whether expected benefits justify any associated risks, or whether traditional methods are preferable for high-stakes or highly sensitive matters

Part II: Vendor Evaluation

Request written responses to the following before making any commitment. Document vendor responses for your records.

Note on negotiation realities: With major AI vendors, many contract terms may not be individually negotiable. Enhanced protections may be available only through enterprise tiers or may not be available at all. Evaluate what protections are actually achievable before committing to use with sensitive client information.

Data Practices

Understanding how a vendor handles your data is critical to protecting client confidentiality and complying with your professional obligations.

- ☐ Determine whether your input data will be used to train or improve AI models. This is the threshold question for use with confidential client information.
- ☐ If data is used for training, determine whether you can opt out, whether opt-out is automatic or requires action on your part, whether opting out affects functionality or cost, and whether it applies to data already submitted (potentially relevant when reassessing existing tool use).
- ☐ Determine whether your input data will be used for any purpose other than generating outputs for you (such as analytics, product improvement, or research) and whether the vendor retains the information. Consider ER 1.6 constraints.
- ☐ Determine whether the vendor retains your outputs and for what purposes.
- ☐ Determine what metadata or derived data is created from your usage and how it may be used.
- ☐ Inquire about the information sources the tool uses to generate outputs including training data, retrieved sources, and any integrated databases. Assess whether these sources are appropriate, current, and reliable for your intended use cases. Ask how frequently information is updated, as currency requirements vary by practice area (rapidly evolving areas like tax or healthcare regulation may require more current information than established common law areas).

Output Quality

- ☐ Inquire about accuracy metrics, error rates, or performance benchmarks for your intended use case. If specific data is unavailable, ask about the vendor's methodology and processes for ensuring output quality and identifying limitations.
- ☐ Determine whether the tool provides features supporting verification of outputs, such as source citations, links to original materials, or confidence indicators. The relevance of specific features depends on your intended use.
- ☐ Request documentation of known limitations, including use cases where the tool performs poorly or is inappropriate.

Security and Compliance

☐ Determine where data is stored and processed, including countries, cloud providers, and data centers.

☐ Review security certifications (such as SOC 2) and request supporting documentation.

☐ Determine the vendor's policy for responding to subpoenas or other legal process seeking customer data, including whether you receive advance notice where legally permitted.

☐ Review business continuity and disaster recovery capabilities.

☐ Determine what happens to your data if the vendor is acquired, merges with another company, or ceases operations.

☐ If you will process regulated data through the AI tool, verify the vendor maintains appropriate compliance infrastructure:

- **Health information**: For processing PHI, verify the vendor maintains HIPAA compliance infrastructure, including certifications and Business Associate Agreements with underlying model providers and subcontractors
- **Financial information**: For data subject to GLBA or financial services regulations, verify appropriate controls and compliance capabilities
- **Personal information**: For data subject to state privacy laws, GDPR, or other privacy regulations, verify compliance capabilities and availability of required agreements
- **Other regulated data**: Identify requirements specific to your practice areas and verify vendor capabilities

Vendor Assessment

☐ Assess vendor reliability and track record:

- Search for reported data breaches, security incidents, or regulatory actions
- Review independent assessments, user reviews, and publicly available feedback
- Check for public complaints with consumer protection agencies
- Seek references from other legal users with similar practice profiles
- Assess vendor financial stability and likelihood of continued operation

Part III: Contract Requirements

Essential Terms

- ☐ Ensure a written contract governs the relationship. Standard terms of service may provide inadequate protection for legal practice use.
- ☐ Ensure the contract prohibits using your input data to train or improve models without your explicit consent.
- ☐ Ensure the contract restricts use of your input data to providing services to you only.
- ☐ Ensure the contract requires the vendor to maintain the confidentiality of your data.
- ☐ Ensure you retain all rights in your input data.
- ☐ Ensure the contract restricts sharing your data with third parties and requires equivalent confidentiality obligations for any necessary subcontractors.
- ☐ Review the vendor's commitment to notify you before responding to legal process seeking your data, where legally permitted.

Data Management

- ☐ Review data retention policies and confirm you can request deletion of your data.
- ☐ Ensure the vendor will return or destroy all your input data, outputs, and any customized models upon termination.
- ☐ Confirm you can obtain written certification of data destruction.
- ☐ Ensure deletion is complete and permanent, including removal from backups, within a specified timeframe.
- ☐ Confirm you retain rights to use outputs generated before termination.

Intellectual Property

- ☐ Ensure you have sufficient rights to use outputs for all intended purposes, including after contract termination.
- ☐ If your data will be used to customize, train, or fine-tune AI models, even for your exclusive use, clarify ownership and your rights to them upon termination.
- ☐ Require the vendor to represent it has obtained all necessary rights to training data and to provide the services.

☐ Require the vendor to defend and indemnify you from claims that the tool itself infringes third-party intellectual property rights.

☐ Understand that most vendors will not indemnify for infringement by outputs. This risk typically falls on you.

Liability and Risk Allocation

☐ Review liability caps to assess whether they provide meaningful recourse given your potential exposure. Caps limited to fees paid in the prior 12 months are common but may be inadequate for significant matters.

☐ Identify excluded damages (consequential, indirect, lost profits, reputational harm).

☐ Understand that most vendors disclaim all warranties about accuracy, completeness, and fitness for purpose. You bear professional responsibility for verification.

☐ Review your indemnification obligations to ensure they are reasonable and do not require you to indemnify the vendor for the vendor's own negligence or breach.

Service and Contract Terms

☐ Review service level commitments for availability, response times, and remedies for failures.

☐ Ensure the contract requires breach notification within a specified timeframe (24-72 hours is typical) and vendor cooperation with your notification obligations.

☐ Inquire about available access controls, permission settings, and audit capabilities. These features support supervision and compliance requirements but may not be available with all tools.

☐ Determine whether the vendor can unilaterally modify material terms (data practices, pricing, core features), with what notice, and whether you can terminate without penalty if you reject changes.

☐ Review termination provisions including transition assistance and data export capabilities.

Part IV: Safe Use and Ongoing Compliance

Verifying AI Outputs

All AI outputs require verification appropriate to their intended use. AI can generate plausible but fabricated content that is difficult to detect without independent review.

☐ For legal authorities: Verify every citation independently. Confirm the source exists, retrieve and review it to ensure it supports the stated proposition, verify it remains valid law, and check any quoted language against the original.

- ☐ For factual assertions: Verify claims against reliable independent sources before relying on them in court filings or client advice.
- ☐ For drafted documents: Review for accuracy, completeness, and appropriateness; verify any stated legal standards or requirements are current; ensure tone and content suit the purpose and recipient.
- ☐ Document verification performed, as appropriate to the matter, including who verified and what steps were taken.
- ☐ Never file any document containing AI-generated content without complete attorney review and verification.
- ☐ Always check to determine whether the Supreme Court or any other court has issued opinions or rules of guidance governing the use of AI. This includes local court rules.

Human Oversight

- ☐ Establish review requirements appropriate to each use, with more rigorous verification for higher-stakes applications.
- ☐ Ensure you can understand and explain the reasoning behind any AI-assisted work product you deliver or file.
- ☐ Never allow AI to make substantive decisions without meaningful human professional judgment.

For non-lawyer use of AI tools:

- ☐ Establish clear policies defining permitted uses, required supervision, and approval requirements.
- ☐ Where available, implement access controls to limit tool access to authorized personnel and uses.
- ☐ Require attorney review and approval before any AI outputs generated by non-lawyers are used externally.
- ☐ Where feasible, maintain audit trails documenting who used tools and what outputs were generated.

Compliance and Recordkeeping

- ☐ Monitor and comply with court rules requiring disclosure of AI use in filings. Requirements vary by jurisdiction and are evolving.
- ☐ Maintain documentation sufficient to respond to inquiries about AI use, including what tool was used, how it was used, and what verification was performed.
- ☐ Establish protocols for client notification about AI use and obtain consent where required by engagement agreements, client policies, or applicable rules.

- ☐ Address how AI use affects billing, including whether efficiency gains are reflected in fees and how AI-related costs are handled.
- ☐ Maintain records, as appropriate to your practice, documenting approved tools, matters involving AI use, verification procedures applied, and training completion.
- ☐ Consider establishing reporting mechanisms for personnel to flag fabricated outputs, errors, or potential security incidents.

Ongoing Monitoring

- ☐ Monitor output quality over time. Model updates may affect performance and reliability.
- ☐ Designate responsibility for tracking developments in AI regulation, court rules, and bar ethics guidance.
- ☐ Discuss AI use with your malpractice insurance carrier to understand coverage for AI-assisted work and any applicable requirements or conditions.
- ☐ Review and update AI policies at least annually, or more frequently as warranted by significant developments.
- ☐ Reassess vendor relationships upon contract renewal, material changes to vendor terms or practices, security incidents, or significant changes to your use patterns.
- ☐ Periodically confirm vendor compliance with applicable regulatory requirements remains adequate.

Note on evolving technology: AI capabilities, vendor practices, and regulatory requirements are evolving rapidly. This guidance reflects current understanding and should be reassessed periodically as the technology and regulatory landscape develop.

Summary

This checklist provides a framework for evaluating GenAI tools consistent with your professional obligations.

Key Principles:

Verification is essential. AI outputs can contain fabricated content that appears authentic. All outputs require verification appropriate to their intended use before external reliance.

Understand data practices before inputting client information. Whether your data trains models for other customers, how it is stored and used, and what protections are in place are threshold questions.

Your professional obligations apply fully. You bear complete responsibility for AI-assisted work product. Competence (including technological competence) confidentiality, supervision, and candor requirements are not diminished by AI use.

Appropriate protections must match your use. Tools and contract terms adequate for non-confidential uses may be inadequate for privileged or regulated information.

The landscape is evolving. AI technology, vendor practices, regulations, and ethics guidance continue to develop. Regular reassessment is necessary.

This checklist is provided for educational purposes and does not constitute legal advice. Practitioners should exercise independent professional judgment and consult applicable ethical rules and opinions in their jurisdiction.

For more formal, legal-focused publications, you may use this version: