



OLD REPUBLIC

GILSBAR



Old Republic Lawyers Professional

Artificial Intelligence for Lawyers: Friend, Foe, or Both?

By Sean Ginty, AVP of Risk Control, Old Republic Lawyers Professional, Inc.

As artificial intelligence (“AI”) becomes more integrated into legal practice, lawyers must exercise care to use these tools responsibly and in full compliance with their ethical duties set forth in the rules of professional conduct. While AI has been available for years, Generative AI (“GenAI”), a relatively new tool, is rapidly transforming legal practice in ways that offer significant benefits but also raise new ethical and professional considerations. GenAI is a type of AI trained on data (text, images, data, music, computer code) that can generate new information, content, and insights. But if the GenAI lacks proper safeguards, it may “hallucinate,” meaning it can provide false information in response to prompts due to its design focus on pattern-based content generation. This article will focus on two critical risks for lawyers: ⁽¹⁾ relying on GenAI-generated outputs without verification and ⁽²⁾ making unauthorized disclosures of client confidences when using GenAI tools.

The Lawyer’s Duty of Truthfulness

A number of the American Bar Association Model Rules of Professional Conduct (“ABA MRPC”) address a lawyer’s duty to be truthful: ABA MRPC 3.3: Candor Toward the Tribunal; ABA MRPC 4.1: Truthfulness in Statements to Others; and ABA MRPC 8.4: Misconduct, which prohibits lawyers from engaging in “conduct involving dishonesty, fraud, deceit or misrepresentation.” Lawyers may violate these rules when they rely on GenAI-generated citations—particularly those that are fabricated—and then file motions or pleadings containing such inaccuracies. Judges nationwide have admonished that AI tools are not a substitute for legal research and that attorneys remain responsible for the veracity of every citation submitted. A claim of ignorance—that the lawyer did not know that the citation misstated the law or was entirely nonexistent—is not a defense.

In a recent federal case in Alabama, a court sanctioned a criminal defense attorney who used hallucinated cases provided by a GenAI tool in motions that he did not verify prior to filing such motions. The court cited a string of

cases involving similar misconduct by attorneys across the country and then listed the harms caused by the use of hallucinated cases in motions before the court, which include:

- wasting the time and money of the opposing party;
- wasting the court’s time and resources;
- causing delays in a case (indeed, the client in the underlying case decided to change counsel due to the use of hallucinated cases, even though the change would significantly delay his own trial);
- causing potential harm to judges and courts that were unfairly identified as being part of the phony court opinions;
- causing potential harm to parties that were unfairly identified as being part of the phony court opinions; and
- causing public cynicism and doubt about the reliability of the judicial system.

¹U.S. v. *McGee*, 2025 WL 2888065 (S.D. Ala. October 10, 2025)

As part of the lawyer's sanction, the court ordered him to file a copy of the court's opinion in all matters where he appeared as counsel and final judgment had not been entered, as well as in any court wherein he appears as counsel for twelve months after the date of the court's order. The lawyer was also ordered to provide a copy of the order to any jurisdiction in which he was licensed to practice law.

To meet these obligations under the ABA MRPC, lawyers must understand the limitations of GenAI tools. Law firms may want to consult with legal-tech specialists, consider bar association guidance, and draw on peer experience to determine which GenAI tools best fit their needs. While GenAI tools can assist with idea generation and preliminary drafting, they cannot replace independent legal judgment. Nor can attorneys outsource their responsibility to file truthful and accurate pleadings to GenAI. Lawyers should treat GenAI tools as they would an inexperienced law clerk. Lawyers must verify every case citation, statute, or regulation provided by a GenAI tool to ensure compliance with ethical duties.



Safeguarding Client Information

Another significant risk arising from the misuse of GenAI tools is the potential inadvertent disclosure of client information when documents containing such information are uploaded to an open GenAI platform. Many public or free GenAI programs reserve the right to use submitted information to train their models, creating a real possibility that client information could later appear in responses

to other users. Courts may also determine that uploading confidential material to an open platform constitutes a waiver of attorney-client privilege.

ABA MRPC 1.6 requires lawyers to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Fortunately, lawyers can still benefit from GenAI tools while minimizing the risk of disclosure.

Law firms should carefully review any GenAI platform's terms and conditions, including its treatment of confidential and private information, prior to inputting any client data. Ideally, law firms should only use a closed GenAI system that is accessible only to a defined community. However, closed systems can be costly and may lack some of the features available in public tools. When using a public GenAI tool, best practices for inputs include:

- Describing issues as hypotheticals;
- Refraining from putting particularly sensitive data in any prompts; and
- Making facts generic enough that re-identification is impossible.

For example, it is acceptable when using a public GenAI tool to input anonymized data and details that protect confidential client information. Conversely, it is unacceptable when using a public GenAI tool to upload entire complaints, medical records, or privileged email chains.

Lawyers should also advise their clients not to use AI tools in connection with their legal matters without first consulting counsel. In a recent New York case², a client generated AI-created documents to analyze potential defense strategies and then sent them to his lawyer. When the government seized these documents during an FBI search, the client argued that they were protected under attorney-client privilege and the work product doctrine.

The court rejected both arguments, holding that because the AI tool was not an attorney, neither the attorney-client privilege nor work product doctrine applied.

This decision underscores the risks clients face when independently using AI tools without legal guidance.

²*U.S. v. Heppner*, No. 25-cr-00503-JSR (S.D.N.Y. Feb. 17, 2026).

Client Consent

Law firms using GenAI should obtain informed client-consent at the outset of the representation and documented in an engagement letter or other writing. Clients should not first learn of the law firm's use of GenAI on their matters through a data-breach notice or another adverse event. One bar association has offered sample language that lawyers may wish to incorporate in their engagement letters:

Use of Generative AI: While representing you, we may use generative AI tools and technology to assist in legal research, document drafting and other legal tasks. This technology enables us to provide more efficient and cost-effective legal services. However, it is important to note that while generative AI can enhance our work, it is not a substitute for the expertise and judgment of our attorneys. We will exercise professional judgment in using AI-generated content and ensure its accuracy and appropriateness in your specific case ³

AI Recording Tools

Many law firms use AI-based recording tools to generate summaries of audio and video conferences. Although this practice may appear routine, it presents several risks that lawyers must evaluate before adopting such tools. Key considerations include:

- the AI tool's and provider's terms of service;
- the privacy and security measures used to safeguard data;
- where the data is stored and the duration of retention;
- whether the recorded data may be discoverable in litigation;
- whether the AI tool or provider uses the data for model-training purposes;
- the law firm's ability to delete the data upon request; and
- whether the law firm can disable the tool's recording function as needed.⁽⁴⁾



Client Consent and Lawyer Due Diligence

Lawyers must inform clients that they intend to use an AI system to record any lawyer-client communications and must obtain their consent before doing so. While some clients may welcome a memorialized record of discussions, others may prefer not to be recorded. Being recorded may change or limit how openly clients communicate with their lawyers.

Many GenAI recording systems use voice-recognition technology to identify individual speakers. In jurisdictions with biometric privacy laws, using such technology without the consent of those being recorded may result in violations of those laws.

Additionally, lawyers must carefully review AI-generated summaries or transcripts. These outputs are often not fully accurate, and relying on them without verification can compromise a lawyer's duties of competence and diligence.

³New York State Bar Assoc. Task Force on Artificial Intelligence (April 2, 2024)
⁴New York City Bar Assoc. Comm. on Pro. Ethics, Formal Op. 2025-6 "Ethical Issues Affecting Use of AI to Record, Transcribe, and Summarize Conversations with Clients."



AI-Recorded Multi-Party Meetings

Lawyers should obtain the consent of all participants before using AI based recording tools in any virtual meeting. While some states permit recording with the consent of only one party, others require all party consent. Even attorneys in a one party consent jurisdiction may violate another state's criminal or civil laws if any participant is located in an all party consent jurisdiction. Securing express consent from everyone eliminates the risk of infringing on others' privacy rights.

Conclusion

Law firms are increasingly leveraging GenAI to enhance efficiency, but attorneys must remain vigilant to the associated risks. Effective use of these tools requires sound risk management practices to ensure that technological gains never compromise lawyer professional conduct and liability standards.

OLD REPUBLIC LAWYERS PROFESSIONAL

Tips for Using Gen AI

- Treat GenAI as an assistive tool, not a replacement for professional legal judgment
- Adopt written GenAI policies governing appropriate use
- Train attorneys and staff on GenAI risks, limitations, and ethical requirements
- Independently verify every case, statute, regulation, rule, and quoted authority provided by GenAI
- Inform clients at the outset that the firm may use GenAI in their matters
- Obtain client consent to use GenAI on their matters and document such consent
- Review GenAI terms on confidentiality, storage, and model-training before entering any client information
- Obtain consent from clients before using any AI recording or transcription system
- Obtain consent from all participants in multiple-party virtual meetings before using any AI recording or transcription system
- Carefully review all AI-generated transcripts or summaries for accuracy

**For more information, contact a Gilsbar representative at
800-906-9654 or [gilsbar.com/contact-us](https://www.gilsbar.com/contact-us)**

Old Republic Lawyers Professional insurance contracts are underwritten and issued by one or more of the following: Pennsylvania Manufacturers' Association Insurance Company; Manufacturers Alliance Insurance Company; Pennsylvania Manufacturers Indemnity Company, rated A+ (Superior) by AM Best. For the latest Best's Credit Ratings, access www.ambest.com.

This material is provided for informational purposes to describe the coverages that Old Republic Lawyers Professional offers. Coverage is subject to underwriting and the applicable policy terms, conditions, and limits. This is not intended to and does not modify the terms and conditions of any insurance policy or imply that any particular claim is covered.