Wolters Kluwer

Expert Insights

AI Tools in Legal Practice and Associated Risks and Mitigation Strategies

By Christopher J. Dufek, Partner, and Aubrianna L. Mierow, Associate, Hunton Andrews Kurth LLP

In just a few years, generative AI technology has begun integrating into workplaces across industries. The legal field is no different as generative AI technology promises to aid attorneys in improving efficiency and conducting essential tasks like research, drafting, and analysis of large document or data sets—a selling point to both law firm leaders and clients alike. Despite the practical benefits and efficiencies created by the deployment of AI platforms, several pitfalls have emerged that must be addressed and monitored carefully. Such pitfalls include maintaining the confidentiality of client information, maintaining privilege over both inputs and outputs associated with AI tools, and ensuring AI's outputs are relevant and accurate.

Deployment of AI at Law Firms

At a high level, AI tools can be broken into public-facing platforms available to the general public (e.g., consumer versions of ChatGPT and Claude), and enterprise versions of these platforms that are generally designed to be operated exclusively by large organizations, including law firms. Enterprise platforms are often integrated directly into the existing business systems to ensure security, data privacy, and compliance with specific requirements unique to the user that are not present on consumer-facing platforms. Importantly, data entered into enterprise platforms is generally not used to educate consumer-facing platform's language learning models ("LLMs"), which preserves confidentiality over the users' information (although the exact terms of each enterprise agreement must be scrutinized on an individual basis). While law firms have access to consumer versions of ChatGPT or Claude, many firms are rolling out enterprise versions of these tools to use for their confidential client work.

The evolution of AI tools has allowed law firms to explore and deploy full suites of AI products that touch on many interrelated aspects of their attorneys' work and practices. While products vary and new products become available on almost a weekly basis, firms generally deploy enterprise AI tools for the following tasks:

- Legal research. AI tools have the ability to analyze prompts and research cases housed on sources such as Westlaw and Lexis.
- Legal writing. AI tools have the ability to prepare first drafts of memos, briefs, correspondence or contracts, among other documents.
- Document review, processing, and summarization. AI tools have the ability to distill large document or data sets into summaries of key facts, timelines and other useful outputs.
- AI notetakers. AI tools have the ability to take real-time notes during Zoom or Teams meetings, among other functions.
- Performance management platforms. AI tools have the ability to track computer activities and may obviate the need for manual tasks like time-entry.
- Agentic platforms. AI tools are capable of building multi-step research and drafting plans, among other functions.

In addition to continuous development of new AI platforms, rules, regulations, laws and ethical requirements that govern the use of AI are similarly evolving at a rapid pace. It is incumbent on law firms and attorneys to monitor these developments closely to ensure their use of AI remains in compliance with the latest mandates by courts and state and federal governments. This article touches on a couple of the evolving areas where attorneys must remain vigilant as AI is deployed in their practice.

Confidentiality of Client Information

Many tools incorporating AI require the input of relevant documents or data to generate the requested output. When this information is confidential to the client or subject to a protective order or confidentiality agreement, it is imperative that attorneys understand what protections (or lack thereof) are in place on the AI platform they are using. For example, client data uploaded to a consumer-facing AI platform like ChatGPT may be used to train the AI's model or be shared unwittingly with third parties either operating or also using the platform. Enterprise versions of these platforms help avoid such disclosures, but the degree of protections vary, and it remains important for the law firms and attorneys to understand what protections are in place and what they can and cannot

©2026 CCH Incorporated and its affiliates. All rights reserved.

do with confidential information on a given platform.

Under the Model Rules of Professional Conduct, which have been adopted in some form by every jurisdiction in the United States, law firms and attorneys have an ethical duty of confidentiality to their clients. [*See* Model Rules of Professional Conduct, Rule 1.6.] Attorneys cannot share information related to the representation of a client without the client's informed consent or implied authorization. [*Id.* at Rule 1.6(a).] Attorneys must take further steps to prevent inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. [*Id.* at Rule 1.6(c).] Therefore, in the context of AI tools where confidential client information may be used, incorporated, or uploaded, attorneys may, depending on the circumstances and risk profile of the tool and information involved, need to (1) obtain informed client consent before using certain AI tools; and (2) ensure that the AI tools are secure and do not misuse information that is deemed confidential by either their client or in the matter they are working on.

Practical steps that law firms can take to protect confidential information while using AI tools include:

- Employ robust training programs for firm employees and attorneys on AI best practices and ethical obligations they have to their clients.
- Review current engagement letters with clients to determine whether the use of AI complies with the scope of representation and update these letters where appropriate to include provisions governing the use of AI with express authorizations from the client for its deployment. Such consent should ensure that the client has knowledge of the risks and benefits of the AI tools the law firm has its disposal, how the AI tools will be used, and why.
- Limit the use of consumer-facing AI tools to strictly public queries that use no case- or client-specific information that could be deemed confidential. Firms should similarly ensure that enterprise AI platforms do not use inputs to train their AI model's algorithm and have stringent confidentiality provisions in place pertaining to data storage and security.
- For each enterprise AI tool, law firms and attorneys should ensure that its data storage and retention policies for uploaded material comply with cybersecurity standards, which could be mandated by the firm, the client, the court, operative protective orders or other agreements, or federal or state governments.
- Block or limit network access to publicly available AI tools that are not customized or authorized for firm use.

Attorney-Client Privilege, Work Product, and Waiver Issues

Incorporating or uploading confidential client information into generative AI tools also raises concerns with respect to maintaining attorney-client privilege and work product protections over uploaded materials, the prompts entered, and the outputs that are created.

Attorney-Client Privilege

At least one court has declined to extend privilege to communications with a publicly available AI tool where no attorney-client relationship existed and there was no reasonable expectation of confidentiality, raising questions about how privilege principles apply in this context. [*See, e.g. United States v. Heppner*, 2026 WL 436479 (S.D.N.Y. Feb. 17, 2026).] In *Heppner*, the Southern District of New York held that a defendant's communications with a publicly available generative AI chatbot were found to be not privileged when (1) no attorney-client relationship existed between the defendant and the chatbot; (2) there was no reasonable expectation of confidentiality, given the AI tool's privacy policy and terms and conditions; and (3) the chats were not directed by counsel or communications for the purpose of obtaining legal advice. [*Id.*] Although *Heppner* contemplated a represented defendant's personal use of publicly available, consumer-facing AI tools, the decision raises important considerations for law firms that deploy enterprise AI tools. Principally, law firms should ensure that all firm-approved AI tools are confidential, not publicly available, controlled by the attorney, and comply with firm cybersecurity practices. It is incumbent on each firm to understand and vet the enterprise agreements they enter into with AI providers, as not all tools (or their underlying agreements) are the same.

Work Product Doctrine

Courts to date have analyzed how far work product protections extend to use of consumer-facing AI tools, and there have been a mix of outcomes depending on the jurisdiction where the matter is addressed. While this is still a developing area of the law, there are some general principles regarding the work product doctrine that can be derived from recent decisions that may have implications on law firm's use of enterprise AI tools. [*See, e.g. Heppner*, 2026 WL 436479 (S.D.N.Y. Feb. 17, 2026); *Warner v. Gilbarco, Inc.*, 2026 WL 373043 (E.D. Mich. Feb. 10, 2026).]

In *Heppner*, the Court declined to extend the work product doctrine to a represented defendant's personal use of publicly available generative AI tools, holding that the chats were not at the direction of counsel and did not reflect counsel's mental impressions or strategy. It also was not clear to the Court as to whether they were prepared in the anticipation of litigation. In *Warner*, on the other hand, the Court held that a self-represented defendant's communications with a publicly available

©2026 CCH Incorporated and its affiliates. All rights reserved.

generative AI chatbot were protected work product when the defendant was acting as his own counsel and the materials were prepared in advance of trial. The Court also noted that the defendant did not waive work product protection when he shared confidential information with the third-party chatbot, finding the decision consistent with case law extending work product protection over an attorney's searches in legal research databases.

Although these cases dealt with whether an individual's generated content from a consumer-facing AI tool was protected work product, their holdings still shed some light on whether a firm's use of enterprise AI tools is protected work product. The *Warner* decision signals that courts may view an attorney's generated work product from an enterprise AI tool in the same way that that courts view work product generated from legal search tools such as Westlaw or Lexis. Assuming courts continue to adopt the *Warner* court's view of AI use, firms can confidently continue their deployment of enterprise AI tool with the understanding that the inputs and outputs will remain protected as work product where the traditional elements are satisfied.

But attorneys need to recognize that this is a quickly evolving area of the law that routinely sees new decisions on these issues. One area that could receive increased scrutiny in the near future is whether AI prompts used to identify responsive documents to be produced in a litigation or prompts used in the preparation of discovery responses would remain protected as work product if the validity of a production or discovery responses are challenged in court. While this is only one of many open questions related to the use of AI in litigation, both individual attorneys and law firms must monitor developments over privilege assertions related to their use of enterprise AI platforms to avoid future issues with waiver.

Responsible and Accurate Use of Generative AI Research Tools

It is well-known that generative AI can be susceptible to hallucinations in its output that, left unchecked, can result in attorneys running afoul of numerous ethics and court rules. Drafting and research AI tools have the potential to hallucinate, or make up, cases that do not exist. This is more pervasive in consumer-facing, LLM AI tools, which generate outputs based on patterns learned during training and, in some implementations, may incorporate information retrieved from external sources, as compared to enterprise AI tools that pull from a limited universe of data (e.g., an AI platform pulling exclusively from cases available on Westlaw or Lexis or from within a law firm database). However, enterprise AI platforms are not fully immune from hallucinations and outputs still must be thoroughly checked.

Hallucinations can take the form of wholly made-up case citations or more nuanced characterizations of a case's holding or facts that could result in inaccurate representations to a court. There are numerous examples of attorneys who incorporate hallucinations into briefs and court filings that have run afoul of ethics and court rules. Courts across the country have held that such an oversight is inexcusable and calls into question a attorney's competence and honesty (even if the attorney signing the brief was not the one who used the AI tool for the research). [*See, e.g.*, *In re Prince Global Holdings Ltd., et al.,* No. 26-10769-mg, Dkt. 25 (S.D.N.Y. Apr. 18, 2026) (law firm apologizing for AI hallucinations in motion); *Anthony C. Hill v. Workday, Inc.*, No. 3:23-cv-06558-PHK, Dkt. 230 (N.D. Cal. Apr. 28, 2026) (imposing admonishment, monetary fines, and four hours of live CLE upon attorney who submitted briefs with caselaw hallucinations); *Kettering Adventist Healthcare v. Collier*, No. 3:25-cv-00273-WHR-CHG, Dkt. 122 (S.D. Ohio Feb. 25, 2026) (finding attorneys in contempt of court and in violation of Rule 11, imposing monetary sanctions, and making bar referral when attorneys used hallucinated cases in brief); *Lifetime Well LLC v. IBSpot.com Inc.*, No 2:25-cv-05135-MAK, Dkt. 42 (E.D. Pa. Jan. 26, 2026) (imposing monetary sanction and requiring contempt order be shared with professional association).]

Each infraction raises unique ethical inquiries under the Model Rules of Professional Conduct. Consequences imposed on attorneys who fail to verify cases produced by AI can include monetary sanctions, bar disciplinary proceedings, and ineffective assistance of counsel claims, among others. To prevent false or inaccurate information from AI being filed in court, law firms should consider:

- Implementing strict training covering both AI use and ethical considerations each attorney must be aware of in connection with its use, including the development of firm policies and guidelines.
- Requiring that any attorney using AI tools disclose to other attorneys on the matter that a portion of the work was aided or created by AI to ensure the appropriate oversight is in place.
- Requiring that attorneys individually verify the AI outputs through cite-checking and proof reading. A good rule of thumb is that any AI output should be treated as a first draft, requiring significant review and revisions before being finalized.

Final Thoughts & Recommendations

As generative AI technology continues to grow, refine itself, and become ubiquitous across workplaces and industries, law firms

©2026 CCH Incorporated and its affiliates. All rights reserved.

must stay abreast of developments that could impact the integration of AI into the practice of law. Law firms who currently use AI, or are thinking of incorporating AI into their practice, should continue working closely with their clients on how it should be deployed in a given matter and work closely with their attorneys and staff to ensure they are properly trained and educated on its use and the ethical obligations that must be met. Each firm should implement strict policies and guidelines on how AI platforms can and should be used and ensure that its attorneys remain up to date on the latest rules, regulations, and laws governing the use of AI. Each AI platform that is rolled out for either internal or client-facing work must be thoroughly vetted to ensure it works as advertised and has robust data and privacy protections in place to preserve the confidentiality of client or case information.

Generative AI tools have the potential to revolutionize the practice of law, but their deployment must be carefully monitored and constantly refined as new products are rolled out. Ultimately, the burden is on both the individual attorney and the firm to ensure the AI platforms being used comply with client requirements, their own ethical obligations, and all other rules, regulations, or laws mandated by courts and applicable state or federal authorities.

©2026 CCH Incorporated and its affiliates. All rights reserved.