

NEWS

Avoid Use of AI that Will Waive the Attorney-Client Privilege

September 18, 2026 | [Allen Smith, J.D.](#)



The use of [artificial intelligence - \(<https://www.shrm.org/topics-tools/workplace/ai-workplace-common-use-cases-practical-applications> \)](https://www.shrm.org/topics-tools/workplace/ai-workplace-common-use-cases-practical-applications) (AI) is accelerating efficiencies at workplaces but is not without risks when preparing for potentially litigious steps such as hiring decisions or termination. Its use in this legal context, particularly through publicly available and unrestricted platforms, can lead to the waiver of the [attorney-client privilege - \(<https://www.shrm.org/topics-tools/news/managing-smart/attorney-client-privilege-need-to-know> \)](https://www.shrm.org/topics-tools/news/managing-smart/attorney-client-privilege-need-to-know) and work-product protection under certain circumstances. The implications of this burgeoning area of the law for organizations extend beyond appropriate policy implementation to awareness among employees and HR.

“The challenge is that many people don’t think of their AI chat history as something that could surface in litigation, but it absolutely does,” said Jason Stavely, an attorney with Quarles in St. Louis and San Diego. “Just like [email - \(<https://www.shrm.org/topics-tools/news/managing-smart/communications-platform-right-team> \)](https://www.shrm.org/topics-tools/news/managing-smart/communications-platform-right-team) communications, chat histories create potentially relevant and discoverable information.” Discovery in litigation is the pretrial process where each side gathers and exchanges relevant information, documents, and evidence to prepare its case.

Fast-Evolving Area

Whether the attorney-client privilege or work-product doctrine apply to the discoverability of AI in litigation “is a fast-evolving area,” said Bradford Newman, an attorney with Eversheds Sutherland in Silicon Valley, Calif.

Moreover, it varies by jurisdiction — as a result, the best practice is checking with counsel before using AI in litigation-related scenarios, said Keia Atkinson, an attorney with Fisher Phillips in San Diego.

Attorney-client privilege protects communications between a client and their attorney made in confidence for the purpose of obtaining legal advice, noted Marcia Wagner, an attorney with The Wagner Law Group in Boston. The work-product doctrine protects documents prepared by or at the request of counsel in anticipation of litigation or for trial, as well as documents reflecting the attorney’s litigation strategy, she added.

Conflicting case law in federal district courts thus far about when the use of AI waives the attorney-client privilege and protected work product “are merely the first wave of cases to analyze these questions,” Newman said. Circuit law by federal courts of appeal throughout the country ultimately will develop further. “Ultimately, it is likely that the Supreme Court weighs in on these important issues,” he said.

Limit Use of AI with Respect to Litigation

Employers’ AI chat history that must be shared with opposing counsel during the discovery process of litigation could result in employer liability.

For example, if an AI system picks up that an individual’s age was considered in connection with a hiring or termination decision, a bad document trail has been established, according to Frank Palmieri and Jason Lacey, attorneys with Palmieri & Eisenberg in Princeton, N.J.

If an HR professional uses AI to draft talking points for a termination meeting, or a supervisor asks an AI tool how to handle a problem employee, those prompts and responses could be discoverable, Staveland said.

“Employers should assume that chat histories on publicly available AI platforms are not protected by the attorney-client privilege and/or work-product doctrine, and are subject to discovery in litigation,” said Sandra Khalili, an attorney with Greenspoon Marder in Los Angeles.

Employers should implement policies limiting AI use, monitor AI use, and ensure that questions about legal matters are not posed to AI unless under the direction and oversight of an employer’s attorney, she added. Khalili also recommended that organizations impose strict safeguards to preserve confidentiality of chat histories and limit their preservation.

Enterprise platforms are designed to keep prompts, responses, and accessed data within the organization's own environment and are not used to train external AI models, Stavelly noted. That kind of architecture is much more defensible from a privilege standpoint because the data isn’t leaving the company’s control. Compare that with consumer AI tools where the terms of service might allow the provider to access, store, or even use an employer’s inputs for model training, he added.

When someone uses AI as part of seeking legal advice or preparing for anticipated litigation, the chat history could contain privileged or work-product-protected material, Stavelly said. But whether that protection holds depends on whether the AI platform itself is treated as a third party that breaks confidentiality, he added. This is why the AI platform choice and company policies become critical.

Alex Karasik, an attorney with Duane Morris in Chicago, agreed that as a best practice, HR should use closed enterprise AI tools to mitigate potential waiver disputes.

That said, “even chat history on an enterprise or closed-system AI can be discoverable if it was not privileged to begin with,” Khalili cautioned. That means that chat history regarding inquiries made by employees about legal questions before retaining counsel is subject to discovery.

“Those inquiries will contain facts and concerns that would be disastrous to disclose to opposing counsel,” she said. “Thus, whether by causing the unintentional waiver of privilege or by allowing discovery of the employer’s confidential concerns, the use of AI by employees without proper safeguards can lead to greater liability and higher costs of defense and settlement.”

Newsletter: Subscribe to Workplace Compliance News - (<https://www.shrm.org/topics-tools/news/hr-newsletters>)

Policies Can Provide Guardrails

Employers should implement [policies - \(https://www.shrm.org/topics-tools/tools/policies/simple-ai-governance-policy-employers \)](https://www.shrm.org/topics-tools/tools/policies/simple-ai-governance-policy-employers) governing the use of AI tools in connection with actual or threatened litigation and internal investigations, Newman said. He added that when it comes

to chat histories, the use of AI tools, prompts, and outputs might be deemed discoverable, especially when not done at the direction of counsel.

“The best policies I’ve seen do a few things,” Stavelly said.

First, they mandate that employees use only approved, enterprise-grade AI platforms, including tools where the data stays within the organization’s security perimeter and isn’t used to train external models.

Second, they require [human-in-the-loop - \(https://www.shrm.org/topics-tools/news/keep-humans-in-the-loop-for-successful-ai-adoption \)](https://www.shrm.org/topics-tools/news/keep-humans-in-the-loop-for-successful-ai-adoption) validation for critical decisions, so AI recommendations don’t go unchecked.

Third, the policies address the [bring-your-own-device problem - \(https://www.shrm.org/topics-tools/news/technology/the-workplace-security-risk-of-bring-your-own-ai- \)](https://www.shrm.org/topics-tools/news/technology/the-workplace-security-risk-of-bring-your-own-ai-) — personal devices loaded with consumer AI apps present a real risk when employees use them for work-related tasks.

“Good policies make clear that employees should not input confidential, privileged, or sensitive company information into unapproved AI tools,” Stavelly said. “The key is making sure practice actually matches policy. A policy on paper doesn’t help much if nobody follows it or knows about it.”

Was this resource helpful?

[Leave Feedback](#) >