



Shining a Light on Shadow AI Use

It is an organization's worst nightmare: highly confidential client data and projections for next quarter's earnings were leaked to a third party. The accidental leaker? A dedicated employee. The recipient of this sensitive information? ChatGPT.

It is almost certain that employees at every company have tried or are actively using artificial intelligence (AI) tools at work. Without guidelines and oversight, the risks can be significant. We strongly recommend that every organization take a proactive approach towards internal use of AI and adopt an AI acceptable use policy.

What are AI tools?

Powered by the advent of Large Language Models (LLMs), we are in the midst of an explosion of artificial intelligence use. Consumer AI tools such as ChatGPT, Grok, Claude, and Gemini can write articles, generate images, and even create videos. Enterprise AI tools such as Fireflies, Otter, and Fathom can take notes during virtual meetings and create call transcripts. Both types can summarize documents, draft emails, create slides for presentations, and so much more.

What are the risks?

While AI tools can present great benefits to organizations that deploy them, unsanctioned and unsupervised use of such tools (known as "shadow AI") can lead to issues spanning from copyright infringement to discrimination claims. Furthermore, California, Colorado, Utah, and Texas have all passed regulations governing the usage of AI, with additional state and local proposals on the table.

Data Privacy

It is important to understand that generative AI tools constantly seek new data to help improve and update their datasets. Free or even paid versions of these tools can analyze any inputted information, incorporate it into the underlying model, and provide as an output for all users.

If an employee enters confidential company information into a free version of a generative AI tool (e.g., ChatGPT) it is possible that information may be accessible to other uses of the tool.

Inaccuracy & Hallucinations

While AI tools can produce results that may seem incredible upon first glance, forgetting to double check the accuracy of the output is a major mistake. Attorneys across the country have been sanctioned by judges for submitting pleadings to the court citing fictitious cases or inaccurately stating the outcome of previous rulings. Employees run the risk of factual error when they use AI to summarize large documents or synthesize research.

Employment & Human Resources

With respect to employment-related decisions, anti-discrimination laws still apply even when deploying an AI tool that claims to be “unbiased.” An internal recruiter might turn to an AI tool to help wade through hundreds of resumes. However, this tool could unfairly discriminate against candidates of color if its training data reflects historic biases and open the company up to a lawsuit.

HIPAA

Reporting by **HIPAA Journal** in May 2025 showed that 71% of healthcare employees are using personal AI accounts at work. If protected health information is shared with a tool that isn’t HIPAA-compliant and governed by a business associate agreement, this constitutes a HIPAA violation and may draw regulatory scrutiny.

An easy scenario to imagine is an employee using an AI tool to take notes on patient meetings. Assuming there is no business associate agreement in place, each patient meeting incorporating the AI tool constitutes a new breach of HIPAA.

What should your organization do?

Regardless of whether or not they intend to deploy large-scale AI technology, organizations should be creating acceptable use policies for their workforce and educating employees on the potential risks of improper usage. An AI use policy should establish what tools employees are allowed to use (if any) and for what purposes.

If your organization wants to allow employees to use AI tools, we encourage you to enter into an agreement with your preferred vendor and provide employees with corporate credentials rather than having employees use individual memberships which may have more limited data protections.

What's Next?

If you need assistance navigating this new frontier, please reach out to:



**Leah
Irwin**



**Mallory
Regenbogen**



**Alison
Best Lutich**



View all of our Monday Minute issues [here](#).

About Our Firm

For nearly 65 years, Gallagher has been a trusted partner to businesses and non-profits across the Mid-Atlantic region and nationwide. We represent leading universities, hospitals, financial institutions, real estate developers, and more. Our firm is experienced in a wide range of practice areas, including real estate development, affordable housing, civil litigation, confidential investigations,

healthcare, employment law, corporate law, renewable energy, and tax-driven transactions. We pride ourselves on offering innovative, practical solutions with a personal touch, acting as your partner and trusted advisor. With a deep commitment to seeing challenges from every angle, Gallagher is here to help you navigate the complex legal landscape with confidence. For more information, visit www.GallagherLLP.com.

[Join Our Mailing List](#)



218 North Charles Street Suite 400 | Baltimore, MD 21201 US

[Unsubscribe](#) | [Update Profile](#) | [Constant Contact Data Notice](#)



Try email & social marketing for free!