



LEGAL UPDATES

Is AI Putting Your Organization at Risk?

09/16/2024 | 6 minute read

AI tools often drive efficiency and save money, but they have drawbacks. Here's what to know.

Business leaders are considering new AI tools that grow more sophisticated each day. For organizations on the lookout for innovative and tech-enabled cost savings, AI can offer a competitive edge by taking on administrative tasks, speeding up the creative process, and analyzing data. Early adopters also benefit by learning along with their AI tools. Businesses that forego AI altogether, on the other hand, risk being left behind.

As an emerging technology, AI is rapidly improving, but you cannot blithely take your hands off the wheel when you implement it. Like any new tool, AI can present unexpected legal, reputational and practical risks. This is especially true for health care and nonprofit organizations that face unique legal and constituent considerations. Below, we consider three real-world AI use cases that illustrate these hazards for organizations, along with solutions to help leverage AI safely and effectively.

How to Minimize Risks for 3 Common AI Uses

Three common AI use cases for organizations include real-time notetaking, drafting policies, and interacting with customers, clients, patients or donors. Each use poses unique and critical risks with respect to privacy violations, compliance problems, and cybersecurity threats, which often stem from a lack of understanding or appreciation for how these tools work.

AI Notetaking & Transcription

AI notetaking and transcription is both a popular and relatively straightforward use case, allowing call participants or clinicians to more actively engage in the conversation without scrambling to catch every word. Such tools both transcribe what's discussed and can also generate notes, summaries and action items. Notetakers no longer need to join a call just to transcribe the conversation, freeing them up for other tasks and greater productivity. For healthcare providers, these

Related People

Sarah Duniway

Partner

Minneapolis

612.632.3055

sarah.duniway@lathropgpm.com

Kathleen Fisher Enyeart

Counsel

Kansas City

816.460.5843

kathleen.fisherneyeart@lathropgpm.com

Edward (Teddy) J. Fleming, V

Counsel

St. Cloud

320.202.5322

edward.fleming@lathropgpm.com

Tedrick A. Housh, III, CIPP/US, CIPP/E

Partner

tools can allow clinicians to focus on patient care and save time on tedious data entry into medical records.

Yet organization leaders should think carefully before turning on an AI transcription or summarization tool—especially during sensitive discussions. These tools may pose privacy risks in such conversations, particularly if the tool’s vendor has access to the recordings and notes for training purposes. Improper storage of that information also raises the specter of data leaks if the vendor’s cybersecurity is breached. There may also be requirements for participants’ consent to the recording. For health care and human services providers, if the tool will have access to patient or client information, HIPAA likely requires a business associate agreement with the vendor and assurances that the vendor’s data security practices meet HIPAA and HITECH standards. There are additionally a myriad of new state privacy laws for sensitive healthcare services such as behavioral health or reproductive care to consider.

A critical example is using AI notetaking and transcription tools in board meetings where sensitive proprietary data or even legally privileged communications may be discussed. Doing so can lead to serious unexpected consequences later if there is a merger or sale transaction or in the event of a lawsuit. These recordings and summaries may be discoverable in the due diligence or litigation process.

A human scrivener might (and should!) employ discretion to omit sensitive or unnecessary details or note in board minutes when an executive committee is in closed session. Not understanding this nuance, AI does what it was designed for: transcribing verbatim and producing comprehensive summaries. AI-generated notes can also contain errors regarding the content discussed, causing the organization to rely on erroneous data in making a decision. For these reasons, a human should review AI transcriptions for notes of key meetings.

—

Before incorporating AI tools in sensitive situations like board meetings or HR calls, make sure to understand how the tool works, how the vendor stores and uses data, and the potential downstream legal risks if this information is disclosed to outsiders.

—

Likewise for healthcare providers, it is essential that AI generated entries into medical records are reviewed for accuracy as mistakes could lead to serious medical errors like a failure to note drug allergies, improper dosing or treatment plans. Understanding the vendor’s data privacy and cybersecurity practices is critical for protecting patients’ privacy rights.

Policy and Document Drafting by AI

The impulse to let AI draft a document you would otherwise seek from an attorney is understandable. After all, ChatGPT passed a bar exam, right? Indeed, many law firms are looking at ways to implement AI for basic legal tasks. For now, however, ChatGPT and other generative AI platforms—especially those that are free and general purpose—tend to make poor lawyers.

For example, a business asking AI to write a website privacy policy for its customers would hope to save time and legal expense. Unfortunately, the “dumb” nature of AI will likely surface: it does not know your business. Even if you specify an industry, it will generate what it considers the average of all privacy policies—one that does not account for where your organization operates, the data it processes, the products or services it provides, or the unique considerations of your industry. In other words, AI may be capable of generalizing, but not customizing, a legally sound policy for your business. Generative AI can also hallucinate, producing clauses that have no place in a legal document.

Like meeting transcriptions and notes, a misworded policy and disclosure can have expensive legal and reputational consequences. What’s more, a lawyer is likely to spend more time reviewing and editing AI-drafted material (perhaps rewriting it entirely)—making cost savings negligible.

Additionally, no matter who drafts a document using an AI platform, if the user enters confidential or trade secret information, it could become public. An organization could find its trade secrets at risk if it fails to reasonably protect such information through adequate guidance to its employees.

To mitigate such risks, an organization can prohibit use of such platforms altogether or preclude the entry of any personal, confidential or trade secret information. Similarly, if the platform is not HIPAA compliant, an organization could prohibit the entry of patient or client information. Even then, if any patient data would be disclosed, a business associate agreement may be required.

Proprietary or closed platforms may present fewer risks, but unless it has a treasure trove of first-party data on its hands, most organizations are unlikely to set up a proprietary AI platform of their own. That option may prove more feasible as technology continues to advance.

—

Consider whether generative AI is capable of the task at hand. Highly complex and nuanced work products (especially those with legal impacts) should be undertaken carefully, with close human supervision, and might be better left until AI technology advances further.

—

Augmenting marketing and stakeholder interactions

Organizations looking to save on marketing costs and boost response times with customers, clients, patients or donors might be tempted to turn to AI for help. Generative AI-enabled chatbots (like those using Claude, Gemini, and ChatGPT) could assist stakeholders with routine issues and save human resources and customer service personnel for more complex problems. AI-generated images, for example, could cut costs and help market products more creatively.

Remember, however, that as convincingly human as AI chatbots can seem, they can struggle with emotionally charged situations, like when a customer is frustrated. Importantly, they can even give incorrect responses due to hallucinations—which could cost an organization financially and reputationally, as [Air Canada](#) recently discovered when forced to honor an AI-hallucinated discount. These chatbots can also be hacked, creating legal risks if sensitive customer, patient, client, donor, or employee information is accessed by cybercriminals. Additionally, be aware that many jurisdictions are enacting laws requiring notice to consumers to notify them when interacting with AI like chatbots to protect consumers.

Marketing and fundraising uses also require caution. An organization with a sterling reputation and trusted relationship with its stakeholders could put that goodwill in jeopardy if AI-generated marketing or fundraising images prove misleading about the nature or quality of its programs or services, or make claims that are obviously false. Legally, regulators like the Federal Trade Commission or a state Attorney General may also investigate deceptive or manipulative marketing or fundraising materials generated by AI—even if it was unintentional. Businesses will be held accountable for mistakes created by AI tools they enable.

Text marketing or fundraising campaigns could also incur fines (and customers' ire) if AI tools send autodialed messages without prior express written consent, further emphasizing the importance of close human supervision.

—

Put AI use policies in place and keep a close eye on generative AI outputs for accuracy and compliance with applicable regulations. Consider whether the use of these tools aligns with the organization's culture and whether it could imperil longstanding stakeholder relationships.

—



Put AI Guardrails in Place Now

There's no doubt that AI tools can be a real asset for organizations and that leaders should start evaluating and experimenting with how they can support their business objectives. Just remember to start small, test tools before you integrate them, and prioritize data privacy and security.

Most importantly, understand the risks. Let us help you—Lathrop GPM lawyers are continually reviewing and analyzing AI developments to help organizations stay competitive and compliant.