E-Briefings

VOLUME 21 • NO. 3 • MAY 2024

The Governance Institute

With AI's Benefits Come Risks

By Dan Yunker, M.B.A., Senior Vice President of Risk and Compliance, *Kodiak Solutions*

The benefits of artificial intelligence (AI) to the healthcare industry have been notable and will only grow as these technologies evolve, improve, and become more accepted industrywide. Healthcare providers will continue to see more opportunities to adopt these technologies to improve diagnosis and treatment, enhance patient experience, and drive automations in revenue cycle, clinical documentation, and other areas to improve process and workflow efficiencies.

Any new technology's benefits, however, come with a dose of risks to consider. Kodiak Solutions identified AI and related technologies as one of the top five management risk areas facing healthcare organizations in 2024. The risks were identified using input from executive management and board members at many of the largest U.S. health systems.[1]

Risks associated with AI are on the minds of health system board members for good reason. AI introduces providers to a set of challenges that can inhibit their ability to achieve strategic goals and business objectives related to patient care, operations, regulatory compliance, financial performance, and strategic growth, among other areas. This article looks at some of the main risks associated with AI and strategies for addressing them.

Top Risks Associated with AI

Cybersecurity and Data Privacy

Protecting sensitive information, including patient data, has long been an imperative as providers adopt new technologies. The risks of a data breach are substantial and include

[1] *5 Top Management Risks for Healthcare in 2024*, Kodiak Solutions, January 2024.

significant financial and reputational damage. In recent years, healthcare organizations have become increasingly valuable targets to cyber criminals, as evidenced by the surge in cyberattacks affecting the industry.

Today's criminals are using AI models to automate their data breaching process, essentially allowing them to rapidly create huge numbers of cyberattack attempts. When cyber criminals make manual probes of a provider's system, it might take months or years to achieve a breach. With AI, a breach potentially could take only days or weeks.

The sophistication of AI technology has also resulted in new depths to cyberattacks. For example, with "deep fake" technology, bad actors can use AI to impersonate humans via emails, text messages, phone calls, and even video calls. The imitations often feature individuals who are known to the human who is the cyberattacker's target. Cyber criminals then attempt to influence the target to do something that compromises the organization's environment and data. As another example, public AI tools are vulnerable to being tricked into revealing secrets about themselves or any of their users, opening the door to data and privacy breaches.

Poor Care Outcomes and Potential for Bias

AI and related technologies have the potential to improve patient care via enhanced diagnostic and treatment capabilities. The accuracy and quality of the results an AI tool produces is directly related to the amount and quality of the data used to train it. Insufficient data, poor quality data, or data containing hidden or even purposeful biases can yield errant results.

For example, a clinical AI model based on biased data could result in biased clinical diagnoses for certain patient populations, particularly those that are already underrepresented in healthcare. Or if the underlying data used in these tools becomes compromised, such as via bad actors corrupting the data, incorrect diagnoses and ineffective treatment protocols could result, causing patient harm.

From the implementation of AI and other technologies, providers can expect to achieve greater efficiencies and reduced staffing and operational costs.

Financial and Workforce Challenges

From the implementation of AI and other technologies, providers can expect to achieve greater efficiencies and reduced staffing and operational costs. Use of AI and other advanced technologies will greatly impact how work is conducted in health systems—and by whom. Within an industry already struggling with staffing shortages, AI that innovates financial close, compliance, and audit workflow processes has tremendous potential as a solution to staffing risks and talent gaps. Using AI to transform existing flawed workflow processes that may produce errors in compliance, financial, or other controls could scale these errors at undetected levels and in rapid fashion. As these capabilities are created and deployed, it is increasingly important to use partners that have the knowledge and IT expertise to evolve the AI-driven automations.

Addressing AI Risks

Health system governing boards and senior leadership clearly have a lot to consider regarding the adoption of AI and related technologies. According to 2023 research from the Center for Connected Medicine and KLAS, however, only 16 percent of U.S. health systems have a systemwide governance policy specifically addressing AI usage and data access.[2]

As boards tackle AI and emerging technologies and develop such policies, they should consider the following strategies.

Take stock of AI. It sounds simple, but to understand the risks associated with AI, providers need to know all the AI systems being used within the organization. Staff should compile an inventory that is reviewed and updated as new tools are introduced within the health system.

Weigh the costs and benefits. Before adoption of AI and related technologies, understand all the implications, including how they benefit the organization, patients, and community, and their associated risks.

Prioritize data security. Keeping PHI secure is already a priority for health systems, but AI has made it even more critical. Providers should make sure existing policies for data collection, storage, and processing comply with current federal and state privacy regulations. Update all policies to include best practice guidelines around AI data security, including information about patient consent and notification regarding use of their personal information in AI tools. Review policies frequently to make sure they are keeping up with these swiftly evolving technologies.

Providers also should make sure data privacy policies cover data shared with third-party vendors, including payers. The recent cyberattack on UnitedHealth Group's Change Healthcare illustrated how cyber criminals can gain access to one IT environment as a means to attack larger or more numerous institutions. Communication with third-party vendors is critical in development and revision of all data security policies.

Adopt continuous monitoring for breaches—and of AI data. As noted previously, AI has sped up criminals' ability to stage a devastating attack on a provider's IT environment. Unfortunately, this often means bad actors using AI are outpacing cyberthreat hunters' ability to detect malevolent actions. Moving forward, constant monitoring of the IT environment for AI-related breaches and cyberattacks will be critical to heading off attacks.

> Clinicians should be encouraged to participate in discussions about implementation of AI tools and, when using such tools, should be guided to exercise their own professional judgement before blindly accepting AI's suggestions as the ultimate truth.

[2] *How Health Systems Are Navigating the Complexities of AI*, Center for Connected Medicine, 2024.

In addition, providers should ensure policies exist to monitor how AI tools are trained, including the data used to train them. Clinicians should be encouraged to participate in discussions about implementation of AI tools and, when using such tools, should be guided to exercise their own professional judgement before blindly accepting AI's suggestions as the ultimate truth.

Focus on workforce training. Finally, an unfortunate reality is that humans—and human error—are at the center of almost all problems associated with AI. That means health systems must ensure proper training of their workforce. This includes making sure that staff are trained on AI-enhanced technology and systems and vigilant in the face of the continuously growing threat of cyberattacks. Discussions about safe data handling should feature prominently in all technology-related training.

Staying on Top of AI's Risks—and Opportunities

Transformative technologies are already here in healthcare—and many more are on the way, with all promising to be crucial to success in the coming years. As new opportunities in AI are unveiled, providers will need to be vigilant in identifying and mitigating the risks associated with these technologies. Health system boards play a key role in staying abreast—and ahead—of these risks and opportunities.

Key Board Takeaways

- Take an inventory of all AI and related technologies within the health system.
- Weigh costs and benefits when deciding on adoption of AI, including benefits or disadvantages to patients, staff, and the community.
- Prioritize data security, making sure the health system's policies for data collection, storage, and processing comply with the latest privacy regulations and cover data shared with third-party vendors, including payers.
- Make sure the health system is continuously monitoring for cyberattacks and prioritizes monitoring quality and accuracy of the data used to "train" AI tools.
- Focus on workforce training in use of AI tools, safe data handling, and how to recognize cyberthreats or attacks.

TGI thanks Dan Yunker, M.B.A., Senior Vice President of Risk and Compliance for Kodiak Solutions, for contributing this article. He can be reached at dan.yunker@kodiaksolutions.io.