COSMOS
Navigate the Compliance Universe

Compliance Today - April 2025

Barry Mathis (bmathis@pyapc.com) is a Consulting Principal at PYA P.C. in Knoxville, TN.

Artificial intelligence: A double-edged sword for healthcare

by Barry Mathis

Introduction: Benefits and threats of AI in healthcare

Artificial Intelligence (AI) is the computerized simulation of human intelligence in machines to perform tasks like learning, reasoning, and problem-solving. The rise of AI has brought immense opportunities and challenges to the healthcare sector—particularly concerning data privacy, security, and compliance. As healthcare organizations become increasingly data-driven, leveraging AI to enhance efficiency, diagnosis, and patient care, they also face a new wave of sophisticated cyber threats. From dark web tools like FraudGPT and WormGPT that weaponize AI to generate malicious code to phishing campaigns enhanced by AI-generated content, the landscape for healthcare compliance and security has grown complex.

This article delves into the dual-edged nature of AI in healthcare, exploring how it can be both an ally in strengthening defenses and a tool for attackers; it offers insights into how compliance professionals can navigate this dynamic landscape.

The bright side: Benefits of AI in healthcare compliance and security

AI's potential to enhance healthcare operations is undeniable. AI can optimize workflows, assist in diagnostics, and enable precision medicine. Specifically, AI holds promise in healthcare data security and compliance in several ways:

- Enhanced threat detection: AI-powered tools can quickly analyze vast amounts of data, identifying anomalies or potential security threats before they escalate into breaches. By leveraging machine learning models trained to detect deviations from the norm, healthcare organizations can proactively address threats.
- Automated compliance monitoring: Regulatory compliance requires stringent monitoring—especially concerning sensitive healthcare data under frameworks like HIPAA. AI can automate aspects of compliance by continuously monitoring systems, flagging noncompliant activities, and suggesting corrective actions. This automation can reduce human error and ensure adherence to regulatory standards.
- Predictive analytics for risk management: AI's ability to analyze historical data can be used for predictive analytics, allowing healthcare organizations to identify vulnerabilities before they are exploited. This analysis is especially beneficial in risk management, where understanding potential threats and mitigating them proactively can safeguard patient data and organizational reputation.
- Streamlined identity and access management (IAM): IAM is a framework of policies and technologies that ensures the right individuals and entities have appropriate access to resources. AI can bolster IAM systems by implementing analytics that verify user identity based on behavior patterns, such as log-in times and

locations. This behavior-based process makes it more challenging for unauthorized individuals to access sensitive healthcare data—even if they possess legitimate log-in credentials.

The dark side: Weaponized AI

While AI has transformative potential for positive applications, it also presents a range of threats, especially as it becomes more accessible on the dark web. Among the tools that exemplify the dangers of weaponized AI are FraudGPT and WormGPT.

- FraudGPT: This tool—available on the dark web—is designed to enable malicious actors to generate highly effective phishing campaigns and social engineering tactics. By leveraging a large language model (LLM), FraudGPT can mimic human-like language and adapt messages based on context, making phishing emails more convincing and personalized. FraudGPT can be particularly concerning in healthcare, where employees may be more vulnerable to phishing attacks disguised as patient or insurance communications.

- WormGPT: WormGPT represents a more overtly malicious application, allowing attackers to automate the creation of malware and other harmful code. By using an LLM specifically trained to understand and create code, WormGPT enables individuals without extensive coding knowledge to launch cyberattacks. This threat poses a significant risk in healthcare, as even lower-level hackers can create ransomware or other malware targeting healthcare systems, often compromising patient data and critical operational systems.

- AI-generated phishing campaigns: Attackers can now use AI to conduct advanced phishing simulations and campaigns. By analyzing healthcare-specific language and organizational hierarchies, AI can generate messages that closely resemble internal communications. For instance, an AI-driven phishing email could convincingly appear to be a directive from hospital administration asking employees to click on a malicious link. This level of realism—coupled with AI's ability to generate thousands of unique messages at scale—significantly increases the threat level for healthcare institutions.

Webinars and training: A double-edged sword

Webinars are a common tool used to educate healthcare professionals about compliance, data security, and regulatory changes. Malicious actors, however, have started using AI to create highly realistic webinars and training sessions designed to harvest information from unsuspecting users. These AI-generated sessions are often difficult to distinguish from legitimate ones, and attendees may inadvertently reveal sensitive information or install malware on their systems.

Healthcare organizations should ensure all webinar content is verified and originates from trusted sources, and they should consider implementing additional authentication steps for accessing sensitive sessions. As phishing campaigns become more sophisticated, healthcare institutions should employ continuous training that specifically addresses AI-enhanced phishing threats.

Healthcare AI applications: Defensive strategies against AI-driven attacks

Despite these threats, AI also has the potential to strengthen healthcare cybersecurity. Some key applications include the following:

- AI-driven threat intelligence: Modern AI tools can analyze data from multiple sources—social media, dark web forums, and threat databases—to predict potential attacks. This intelligence allows healthcare organizations to stay a step ahead of threat actors, deploying countermeasures before attacks are launched. Additionally, AI-driven monitoring tools can alert security teams to unusual activity patterns, providing real-time protection.

- Behavioral analysis for intrusion detection: Leveraging AI to analyze employee behaviors, such as log-in times, locations, and typical usage patterns, can help identify intrusions. For instance, if an employee's credentials are used to access systems at odd hours or from an unusual IP address, AI can flag the activity and prompt further investigation, potentially preventing breaches.
- Automated incident response: AI-powered incident response platforms can automatically assess the nature and severity of a security incident, deploying appropriate countermeasures. In cases of ransomware, for example, AI can isolate affected systems from the network and prevent the malware from spreading further. This ability to respond in real time minimizes the potential impact of AI-driven attacks like those generated by WormGPT.
- Managing multiple security threats: In healthcare, attacks can come from many places at once, like emails, network activity, or smart devices. AI-driven security systems can monitor multiple endpoints—email, network traffic, cloud applications, and Internet-of-Things devices—enabling a unified approach to threat management. This consolidation improves efficiency and enables rapid, coordinated responses to threats.

Data protection: Following the rules in the AI era

The dynamic nature of AI introduces a new layer of complexity to regulatory compliance in healthcare. As organizations adopt AI, they must ensure they adhere to data protection regulations like HIPAA, the Health Information Technology for Economic and Clinical Health, and the General Data Protection Regulation (for international institutions). Compliance professionals should focus on the following:

- Data governance: AI models—especially LLMs—require vast amounts of data, including potentially sensitive patient information. Healthcare organizations should establish strict data governance protocols, ensuring AI tools do not inadvertently access or expose patient data in violation of privacy laws.
- Transparency: Compliance teams should ensure any AI models used for decision-making in patient care or operations are transparent and explainable. Regulators are increasingly concerned about the "black box" nature of AI, and healthcare organizations should be prepared to demonstrate how AI decisions align with privacy and ethical standards.
- Ethical use of AI: Given the risks posed by tools like FraudGPT and WormGPT, healthcare organizations must ensure they employ AI responsibly and ethically. Compliance officers should create guidelines outlining acceptable uses of AI—particularly concerning patient data—and implement robust monitoring to detect any misuse.

Final thoughts

AI represents both a revolutionary tool and a potential threat to healthcare organizations. While AI can improve data security, enhance compliance, and optimize patient care, it also opens the door to increasingly sophisticated cyberattacks, including those driven by tools like FraudGPT and WormGPT. To effectively navigate this dual-edged nature of AI, healthcare compliance professionals must stay informed about their latest developments—both as a tool for innovation and as a weapon for cyber threats.

Compliance professionals can stay ahead by actively participating in healthcare and AI-focused events, such as conferences, webinars, and workshops, to understand emerging trends, regulations, and technologies. Additionally, staying engaged with reputable publications and updates from government agencies, healthcare organizations, and AI-specific journals provides valuable insights. Finally, joining professional networks such as HCCA, online communities, or specialized training programs ensures continuous learning and access to best practices. By

adopting a proactive, multilayered approach to AI security, healthcare organizations can harness the benefits of AI while safeguarding against its misuse, ultimately ensuring a safer environment for patients and providers alike.

Takeaways

- Artificial intelligence (AI)—the computerized simulation of human intelligence to perform tasks like learning and problem-solving—offers both innovation and cyber threats.
- AI can enhance healthcare operations' data security and compliance through better threat detection, automated compliance monitoring, predictive analytics for risk management, and streamlined identity and access management.
- Weaponized AI poses significant threats to healthcare institutions, such as FraudGPT, WormGPT, and AI-generated phishing campaigns and webinars.
- AI can strengthen healthcare cybersecurity with threat intelligence, behavioral analysis for intrusion detection, automated incident response, and management of multiple security threats.
- Organizations must adopt data protection and compliance regulations like HIPAA, the Health Information Technology for Economic and Clinical Health Act, and the General Data Protection Regulation and focus on data governance, transparency, and ethical use of AI.