Importance of Addressing Shadow AI for HIPAA Compliance

Criminal Use of Artificial Intelligence (AI)

Written by Joanne Byron, BS, LPN, CCA, CHA, CHCO, CHBS, CHCM, CIFHA, CMDP, COCAS, CORCM, OHCC, ICDCT-CM/PCS

The process of identifying and containing a breach can be lengthy and expensive, particularly in healthcare, in addition to eroding patient trust. Breaches can disrupt critical healthcare operations, leading to delays in patient care and financial losses due to closing emergency departments and cancellation of appointments. Healthcare providers are legally obligated to notify affected individuals and provide credit monitoring services, which incurs substantial costs. This article addresses AI use by cyber criminals and summarizes 2024-2025 breach findings as reported by IBM's 2025 Report.

Introduction

In 2025, the average cost of a healthcare data breach is $7.42 million, according to a recent report by IBM. Even with a reduction of $2.35 million in breach cost to the healthcare sector, healthcare breaches remain the most expensive of all studied industries for 14 consecutive years! This figure represents a decrease compared to the previous year but still signifies the highest average cost across all industries. The 2025 IBM report, conducted by *Ponemon Institute*, sponsored and analyzed by IBM, is based on data breaches experienced by 600 organizations globally from March 2024 through February 2025.

Shadow AI security incidents cost more - Security incidents involving Shadow AI carried an added cost. They contributed USD 200,000 to the global average breach cost. This higher cost was likely driven by longer detection and containment times for these security incidents, approximately a week longer than the global average.

According to Suja Viswesan, Vice President, Security and Runtime Products, IBM "***The data shows that a gap between AI adoption and oversight already exists, and threat actors are starting to exploit it***."

She also states that "***The report revealed a lack of basic access controls for AI systems, leaving highly sensitive data exposed, and models vulnerable to manipulation. As AI becomes more deeply embedded across business operations, AI security must be treated as foundational. The cost of inaction isn't just financial, it's the loss of trust, transparency and control***."

Employees may turn to Artificial Intelligence (AI) tools to speed up tasks, solve problems, or improve productivity. However, there are risks associated with employees using AI tools, like ChatGPT, Midjourney, or AI-powered assistants, without IT's knowledge or permission, such as Shadow AI being used by criminals. Using AI tools that don't comply with regulations (like GDPR or HIPAA) can result in fines and legal issues.

Shadow AI

Shadow AI refers to the unauthorized use of artificial intelligence (AI) tools and models within an organization, often bypassing IT oversight and security protocols.

AI tools are being used by cyber criminals to launch smarter attacks. Shadow AI tools can introduce unsecured APIs, unmanaged integrations, or other vulnerabilities that attackers can exploit. To reduce the risk of an AI generated attack, it is important to address Shadow AI.

As AI becomes integral to operations, AI security incidents have the potential to disrupt a range of business activities, including compromising sensitive data and disrupting patient care (i.e. ransomware attack locking access to important patient treatment records). IBM's report identifies the following:

- ***Security for AI is lacking***
  The *Cost of a Data Breach Report 2025 – the AI Oversight Gap* quantifies the extent to which attackers are taking advantage of this deficiency and successfully targeting AI models and applications. While the share of breaches involving AI security incidents are small, IBM researchers expect them to grow as AI vendors gain greater market share and penetration into enterprise systems. Shadow AI is of particular concern.

- ***Impacts of security incidents involving Shadow AI***
  Among organizations that experienced a security incident involving Shadow AI, *44% suffered data compromise*. Another *41% reported increased security costs* as a result of those incidents. Operational disruption was more widespread than incidents involving authorized AI. These results suggest Shadow AI incidents have an outsized impact on downstream breach issues that extend beyond data security.

- ***Researchers found 16% of breaches involved attackers using AI***
  Most of these breaches focused on human manipulation through *phishing (37%)* or *deepfake attacks (35%).*

- ***Supply chain compromise was the most common cause of AI security incidents***
  Security incidents involving AI models and applications were varied, but one type clearly claimed the top ranking: *supply chain compromise (30%),* which includes compromised apps, APIs and plug-ins. Following supply chain compromise were *model inversions (24%)* and *model evasions (21%)*. Incidents involving prompt injections and data poisonings made up 17% and 15% of cases respectively.

- ***Unsanctioned AI security incidents were more common than sanctioned AI***
  Shadow AI may go undetected by an organization, and attackers can exploit its vulnerabilities when employees use it. Security incidents involving Shadow AI accounted for *20% of breaches*, which is *7 percentage points higher* than those security incidents involving sanctioned AI. A further 11% of breached organizations were unsure if they experienced a Shadow AI incident.

Foster a Culture of Responsible AI to Reduce Risk

Healthcare organizations can cultivate a culture of responsible AI by prioritizing ethical considerations and extensive workforce training regarding Shadow AI tools and how to avoid an attack. A few tips to reduce risk are listed below.

Build communication with your workforce - Instead of penalizing your workers for using AI tools without permission, find out what they're using and why. Their feedback could be useful in highlighting

the gaps in your ***technology stack*** and governance policies. This allows you to either optimize your workflows or find a way of integrating the tool into them, thereby moving them from unsanctioned "Shadow AI" to legitimate AI tools.

- A modern data stack is a collection of tools and technologies that are used to manage and analyze data in a particular organization or business. It includes various software, programming languages, frameworks, and platforms that can be used to extract, store, process, and visualize data.

Develop Clear Policies - Establish guidelines for AI tool usage, including approved tools and security protocols. This requires interdepartmental teamwork. When integrating AI tools into your business, make sure that IT, operations, and governance departments are aligned.

- For example, operations might want to use the tool in a way that compromises HIPAA security. Another example is when IT evaluates the tool for security but doesn't understand the need for privacy in this assessment, which is the main concern for governance.
- By bringing all these departments together, you will create better policies for responsible AI use and oversight that work for everyone.

Effective Communicate Policies - Provide workforce training and support. Educate employees about the risks of Shadow AI and offer resources for using AI responsibly. By investing in training and education, you inform your workforce of potential pitfalls and consquences. At the same time, you train those unfamiliar with such tools so they can utilize them effectively as well. Whether it's GenAI or AI-powered automation, using it responsibly helps reduce your security vulnerabilities and helps your employees perform better.

Implement Authentical methods - Today, many attackers are logging in rather than hacking in, according to IBM's report. To combat this issue, it's critical to prevent attackers from obtaining those credentials in the first place. One of the most effective ways to do so is by ensuring all human users adopt modern, phishing-resistant authentication methods, such as passkeys. These technologies are designed to eliminate the vulnerabilities of traditional passwords and one-time codes, making it significantly harder for attackers to intercept or misuse login credentials.

Monitor and Manage AI Usage -AI models and applications can pose significant risks if left unchecked. Consider including tools powered by AI and automation which can augment already overburdened security teams. They can significantly reduce the volume of alerts; identify at-risk data; spot security gaps and threats earlier; detect in-progress breaches; and enable faster, more precise attack responses.

Conclusion

The rapid evolution of AI technology presents a challenge to existing regulatory frameworks. Relying solely on HIPAA, not originally designed specifically for AI, leaves gaps in addressing AI-specific risks.

When employees use Shadow AI, healthcare organizations lose visibility and control over how PHI is being accessed, processed, and stored. This makes it difficult to ensure that HIPAA's Privacy and Security Rules are being followed. Shadow AI tools may not have the same robust security measures in place as approved, HIPAA-compliant systems, making them vulnerable to cyberattacks and data breaches. If sensitive patient information (Protected Health Information or PHI) is exposed through these unauthorized channels, it constitutes a HIPAA violation, triggering potential fines legal repercussions and reputational damage. Another consideration is a lack of required Business Associate Agreements. Many

AI tools are developed by third-party vendors. If these vendors handle PHI without a Business Associate Agreement (BAA) in place, another HIPAA enforcement action could be looming as Shadow AI usage bypasses the essential BAA requirement, exposing healthcare organizations to significant risk.

About the author

Joanne Byron, *BS, LPN, CCA, CHA, CHCO, CHBS, CHCM, CIFHA, CMDP, COCAS, CORCM, OHCC, ICDCT-CM/PCS*. Joanne is the Chief Executive Officer of the American Institute of Healthcare Compliance, a *Licensing/Certification non-profit partner with CMS*. She shares her experience of over 40 years as a nurse, consultant, auditor and investigator in the healthcare field.

References

- **IBM Report – *Cost of a Data Breach Report 2025 – the AI Oversight Gap***
  https://www.ibm.com/reports/data-breach

- **IBM – *What is AI TRiSM?***
  https://www.ibm.com/think/topics/ai-trism#:~:text=AI%20TRiSM%2C%20or%20artificial%20intelligence,robustness%2C%20efficacy%20and%20data%20protection.

- **Gartner – *Tackling Trust, Risk and Security in AI Models***
  https://www.gartner.com/en/articles/ai-trust-and-ai-risk

- **Holistic AI – *Shadow AI: Securing Your Business from Unauthorized AI Use***
  https://www.holisticai.com/blog/Shadow-ai#:~:text=Authored%20By,address%20to%20protect%20operational%20integrity.

- **Institute for Experiential AI – Northeastern University - *Expert Insights on Responsible AI Solutions for Healthcare: Best Practices for Implementation***
  https://ai.northeastern.edu/news/expert-insights-on-responsible-ai-solutions-for-healthcare-best-practices-for-implementation#:~:text=Introduction,rather%20than%20compromises%2C%20patient%20care.