A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY MAGAZINE

MAY 2026

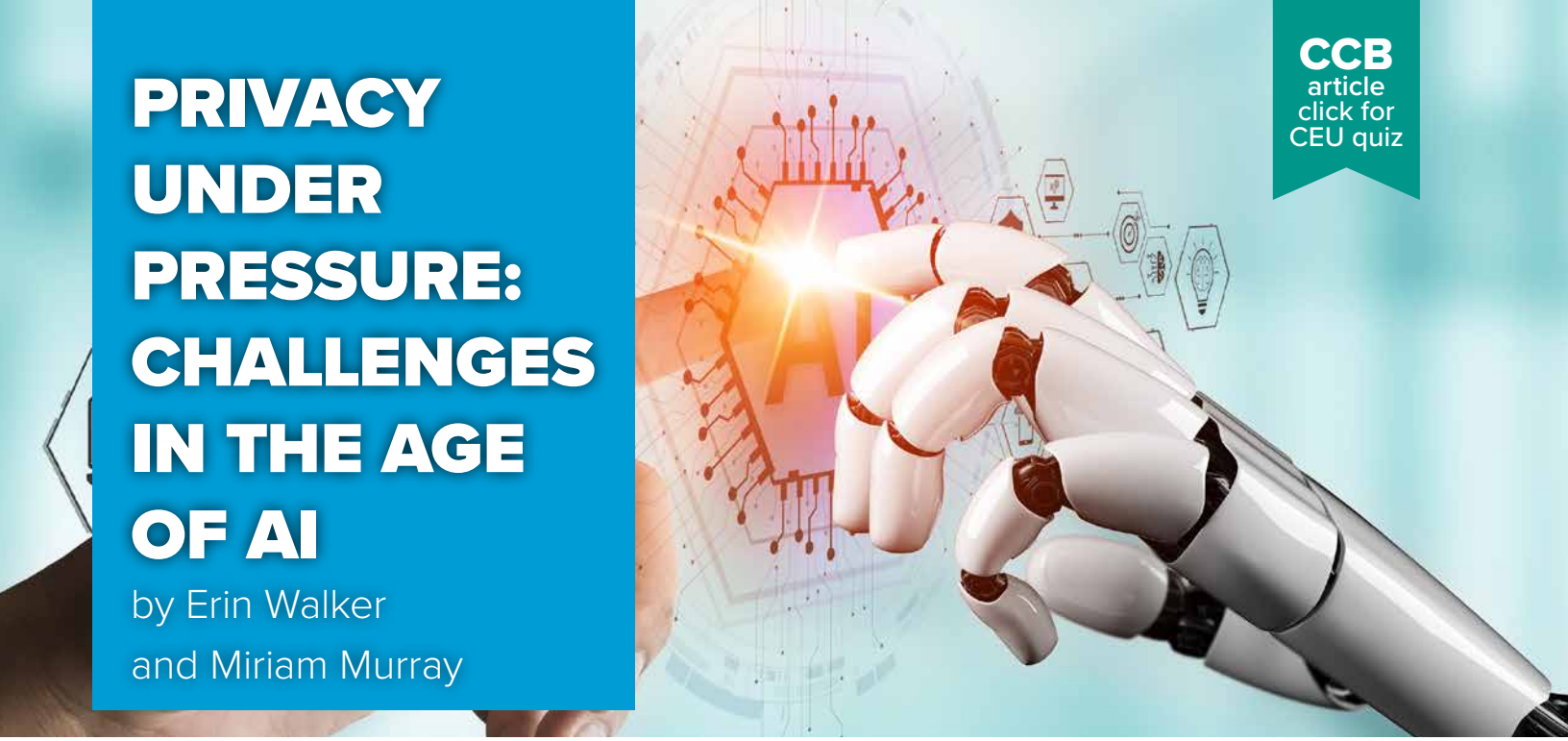
DR. PETER A. KHOURY
DO, MJ, MHA, CHC, CHPC
BOARD ADVISOR AND CHAIR FOR THE HCCA PHILADELPHIA REGIONAL CONFERENCE

HUMAN-CENTERED COMPLIANCE OVERSIGHT THROUGH AI GOVERNANCE (P6)

30 Years HCCA®

PRIVACY UNDER PRESSURE: CHALLENGES IN THE AGE OF AI

by Erin Walker and Miriam Murray



CCB article click for CEU quiz

Erin Walker
(ewalker@pyapc.com) is a Manager at PYA in Nashville, TN.

Miriam Murray
(mmurray@pyapc.com) is a Senior Manager at PYA in Charlotte, NC.

Since its enactment, HIPAA has governed how healthcare organizations, providers, and their business associates (BAs) collect, use, disclose, and secure protected health information (PHI). It is designed to ensure that individuals' health information remains confidential and secure, even as it is shared among authorized parties for treatment, payment, and healthcare operations. With the increased use of AI in healthcare settings, organizations must remain cognizant of the potential privacy risks and violations associated with AI platforms' use of PHI.

The benefits of AI have been widely promoted: It increases efficiencies and puts more knowledge than ever at our fingertips, with the promise of better outcomes and improved patient experiences. Just as healthcare organizations must ensure any other application is used in compliance with HIPAA requirements, they must also ensure the same for AI technologies.

As HIPAA adapts to developments in the AI landscape, one constant remains: The regulations established under HIPAA will continue to be applied consistently. Regulatory agencies expect providers to have a thorough understanding of the AI technologies they use and actively monitor their AI vendors' practices. Therefore, it is critical that healthcare organizations and their BAs understand how these rules apply to PHI being accessed by AI platforms, whether the platforms are managed by healthcare organizations or by one of their BAs.

Regulatory focus

Regulatory agencies are actively monitoring how AI potentially affects healthcare privacy. The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) continues to enforce HIPAA compliance through investigations, audits, and guidance documents, emphasizing the need for organizations to adapt their privacy and security programs to new technologies.

For example, while HIPAA regulations do not explicitly address AI, OCR and HHS have issued guidance on how HIPAA applies to emerging technologies, which includes AI.[1] Similarly, in accordance with the U.S. Department of Justice's (DOJ) *Evaluation of Corporate Compliance Programs,* covered entities are expected to conduct risk analyses accounting for the unique characteristics of AI, such

as data aggregation, automated decision-making, and cloud-based processing.[2]

Beyond complying with HIPAA and other related U.S. federal regulations and guidance, healthcare organizations must also continue to comply with state and international privacy laws. States such as California, New York, and Texas have enacted their own health information privacy statutes, some of which impose stricter requirements than HIPAA.

Safeguards and compliance

The HIPAA Privacy Rule has specific requirements for how PHI may be accessed, maintained, used, and disclosed.[3] Healthcare organizations must determine whether they have the authority to use AI to work with PHI. For example, the purpose of the use must be evaluated, with the results documented and maintained. Is the use for treatment, payment, or healthcare operations, which are permitted under HIPAA? Or is the use authorized, but only with explicit authorization of the individual?

AI technologies often require access to large datasets, which increases the risk of unauthorized access or disclosure of the data if safeguards such as encryption and role-based access controls are not implemented. Another concern is the potential for re-identification of data previously considered de-identified. Even when data meets de-identification standards, advanced AI algorithms can reconstruct identities by correlating patterns across multiple sources.

While the ability to process vast amounts of information drives innovation, it simultaneously heightens privacy risks, making it imperative for healthcare organizations and their BAs to implement adaptive privacy and security programs designed to anticipate and mitigate AI-specific vulnerabilities. While in this new frontier, organizations must continue to ensure that AI tools do not circumvent established privacy protections, such as the "minimum necessary" standard for data use and disclosure.

Safeguarding strategies

Appropriately safeguarding patient privacy has always required a proactive approach, and the same is true for using AI in an organization's privacy program. Healthcare organizations and their BAs must develop and implement specific strategies for addressing the use of AI:

- **Develop an inventory**. Develop a comprehensive inventory of every AI-enabled tool, system, and workflow in use across the organization. This foundational step provides leaders with visibility into where AI is operating, what data it accesses, and how it influences clinical or operational decision-making, so they can determine whether its use aligns with regulatory, ethical, and organizational expectations. An accurate inventory also allows the organization to identify unsupported or "shadow AI" tools, prioritize high-risk applications for review, and assign clear ownership for ongoing monitoring.
- **Conduct risk assessments**. Conduct thorough, AI-specific risk assessments to evaluate how AI systems collect, process, store, and transmit PHI; identify potential vulnerabilities; and assess the likelihood and impact of privacy breaches. Risk assessments should be updated regularly (at a minimum, annually) to reflect changes in technology, data flows, operations, and regulatory requirements.
- **Limit access**. As required by HIPAA's "minimum necessary" standard, configure AI systems to access only the data required for their specific function. Role-based access controls, data segmentation, and automated data minimization tools can help achieve this goal and will assist with reducing the risk of overexposure.

Even when data meets de-identification standards, advanced AI algorithms can reconstruct identities by correlating patterns across multiple sources.

- **Implement system safeguards**. Implement appropriate technical safeguards for protecting PHI in AI environments. Encryption should be applied to data at rest and in transit, ensuring that information remains unreadable to unauthorized parties. Strong authentication mechanisms, such as multi-factor authentication and biometric verification, should also be utilized. Further, to defend against cyber threats, implement a secure infrastructure that includes firewalls, intrusion

detection systems, and regular vulnerability assessments.

- **Conduct regular training**. Train employees on the risks associated with AI, including the potential for inadvertent disclosures, data misuse, and algorithmic bias. Training should include HIPAA requirements and organizational policies and procedures. Training should not be a "one and done" option. Ongoing education and awareness campaigns should be used to maintain a culture of privacy and security and educate workforce members to recognize and respond to potential or actual issues.
- **Continually monitor systems**. Conduct continual monitoring and regular audits of AI systems to detect and address privacy risks.
- **Establish response plans**. Establish incident response plans detailing the procedures for detecting, reporting, and mitigating privacy breaches. Lessons learned from incidents should be utilized to update policies, procedures, and safeguards.
- **Tighten agreements**. Ensure that BA agreements (BAAs) detail the scope of services, data protection requirements, breach notification protocols, and audit rights.
- **Understand third-party practices**. Conduct due diligence on third-party vendors' privacy and security practices to maintain alignment with HIPAA and other regulatory standards.

Risks to monitor

The risks of AI in healthcare are real, especially regarding privacy and security challenges, which highlights the importance of proactive risk management, robust technical safeguards, and continuous oversight. Additionally, as AI technologies continue to evolve, the potential for vulnerabilities will only increase, which will require healthcare organizations and their BAs to ensure their privacy programs are adaptive.

Key concerns organizations should keep top of mind and ensure they are continually addressed and monitored include these risks and others:

- **System security**: Due to inadequate access controls and insufficient oversight, AI systems can expose sensitive patient data. Robust security safeguards are not optional; they must be implemented to ensure appropriate system security.
- **Cybersecurity threats**: Breaches and ransomware attacks continue to exploit vulnerabilities. These attacks disrupt operations and patient care, compromise PHI, and put healthcare organizations and their BAs at risk for regulatory fines, penalties, and reputational damage.
- **Improper use**: Uploading sensitive data to generative AI tools such as ChatGPT and Google Gemini can lead to HIPAA violations. These platforms may not meet HIPAA compliance standards. As an example, Netskope's *Threat Labs Report: Healthcare 2025* found that 81% of data policy violations involved regulated healthcare data, with PHI being the most common type of sensitive data uploaded to unauthorized platforms.[4]
- **AI model training and data re-identification**: AI models trained on patient records can inadvertently memorize and leak sensitive information through specifically crafted prompts, model poisoning (an attack where the training process of an AI platform is intentionally corrupted so that the model learns incorrect, biased, or harmful behavior), and adversarial attacks. Further, recent studies have shown that AI and machine learning can re-identify individuals from datasets previously considered anonymized. For example, a 2024 breach affected 483,000 patients when an AI system linked de-identified data back to individuals, violating privacy requirements.[5]

Recommended policies and procedures

As AI continues to evolve, healthcare organizations and BAs must establish clear policies and procedures for its use. Transparency, such as disclosures about how AI systems use and protect PHI, is key to maintaining trust with patients, regulators, and other stakeholders. A strong AI framework should address issues such as bias and the responsible use of data and align technology with organizational values and community expectations.

To navigate the AI landscape and proactively address privacy compliance, organizations should ensure appropriate policies and procedures are developed and implemented:

- **Risk assessments**
  - Risk assessment policies should include AI-specific factors such as algorithmic decision-making, data aggregation, and potential re-identification risks. Procedures for the assessments should include identifying vulnerabilities in data flows, evaluating vendor

practices, and considering emerging threats such as adversarial attacks. Associated findings and corrective actions should be documented and reported to senior leadership, with assessments updated at least annually or whenever significant changes occur.

- **Technical safeguards**
  - Organizations should develop technical safeguards policies that include procedures for applying encryption to PHI both at rest and in transit to prevent unauthorized access. Use role-based access controls and incorporate multi-factor authentication and monitoring tools to detect issues. A secure infrastructure should include firewalls, intrusion detection systems, and regular vulnerability scans.
- **Third-party vendor management**
  - Per policy, AI vendors should be subject to BAAs and ongoing compliance reviews. Further, BAAs should define responsibilities for safeguarding PHI, breach notification timelines, and audit rights. Additionally, organizations should conduct due diligence before onboarding vendors and require evidence of HIPAA compliance, i.e., security risk assessment reports, privacy/security policies and procedures, and independent auditor confirmation of compliance. Implement periodic vendor compliance reviews and audits to verify adherence to contractual and regulatory obligations.
- **Training and education**
  - An organization's policies should reflect ongoing training and education, scenario-based exercises, and awareness campaigns to reinforce best practices, including HIPAA requirements and AI-specific risks.
- **Reporting concerns**
  - Policies should be established with clear procedures to encourage employees to report concerns and participate in discussions about AI use.
- **Auditing and monitoring**
  - Policies and procedures should outline how and when to monitor regulatory developments, and they should be regularly updated to meet evolving standards. Assign responsibility for tracking regulatory changes and updating organizational policies accordingly.
- **Governance**
  - Through an established AI governance committee, organizations should develop policies and procedures to ensure transparency by documenting how AI systems use PHI and, with guidance from legal counsel, communicating this to patients and stakeholders. CT

Endnotes

1. U.S. Department of Health and Human Services, Office of Inspector General, *General Compliance Program Guidance*, November 2023, https://oig.hhs.gov/documents/compliance-guidance/1135/HHS-OIG-GCPG-2023.pdf.
2. U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, updated September 2024, https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl.
3. U.S. Department of Health and Human Services, "The HIPAA Privacy Rule," content last reviewed September 27, 2024, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.
4. Netskope, *Threat Labs Report*: Healthcare 2025, accessed March 2, 2026, https://www.netskope.com/resources/threat-labs-reports/threat-labs-report-healthcare-2025.
5. Censinet, "HIPAA and the Algorithm: What Happens When AI Gets It Wrong?" accessed March 2, 2026, https://censinet.com/perspectives/hipaa-and-the-algorithm-what-happens-when-ai-gets-it-wrong.

Takeaways

- Maintain a current, organizationwide inventory of all AI systems, including how protected health information is collected, used, transmitted, and secured.
- Monitor evolving federal and state regulatory requirements to ensure AI-related practices stay compliant.
- Develop and adapt privacy, security, and compliance strategies as standards and AI capabilities change.
- Balance the opportunities AI brings to healthcare with the heightened risks it introduces to privacy and data protection.
- Prioritize patient privacy by understanding risks, applying safeguards, and embedding compliance into every stage of AI adoption.