CYBERSECURITY AWARENESS MONTH

CYBERSECURITY RISK EXPOSURES REMAIN HIGH AND COMPLIANCE CONFIDENCE LOW ACROSS THE HEALTHCARE SECTOR

by Lynn Rohland, Darrell Armer and Rachel Poynter

In the fast-paced and critical healthcare services field, patients expect robust adherence to security safeguards for their personal data and electronic protected health information (ePHI). Especially since patient data is essential for continuity of care and maintaining patient trust. However, more than two decades after the Health Insurance Portability and Accountability Act (HIPAA) Security Rule was published, many covered entities and business associates remain non-compliant with the rule, despite operating in a digital 'threatscape' climate consisting of escalating cyber risks. In 2024, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) imposed near-record-level fines for HIPAA violations, underscoring the persistent compliance challenges faced by healthcare organizations.

CYBERSECURITY AWARENESS MONTH

Compliance and Confidence Reach a New Low

- 70% of respondents to HIPAA compliance audits conducted over the last year reported lacking confidence in their ability to effectively respond to today's cybersecurity threats, such as ransomware and phishing attacks.
- Fewer than 40% of covered entities and business associates are confident in their ability to demonstrate HIPAA compliance, despite the standards being decades old, reports the 4th National HIPAA Compliance Survey (2024).
- 20% of respondents to the HIPAA Journal's 2025 Annual Survey indicate they have no confidence in demonstrating compliance, particularly with the Security Rule.

These figures reflect a growing non-compliance posture dangerously out of sync with today's cybersecurity threat landscape. Year over year, the healthcare industry remains a prime target for cybercriminals, driven primarily by the black-market value of medical data, which often garners up to 50 times more revenue than credit card information. Consequently, the current state of the industry shows that the HIPAA Security Rule extends well beyond mere compliance as a formality — it is a vulnerability that cybercriminals are exploiting with ruthless efficiency, including the adoption of AI-powered attacks.

Legal Implications Unfolding

As of October 2025, the HIPAA Security Rule (45 CFR Part 164, Subpart C) has not been substantively updated since the 2013 Omnibus Rule, despite a Notice of Proposed Rulemaking (NPRM) issued by the OCR on December 27, 2024.

CYBERSECURITY AWARENESS MONTH

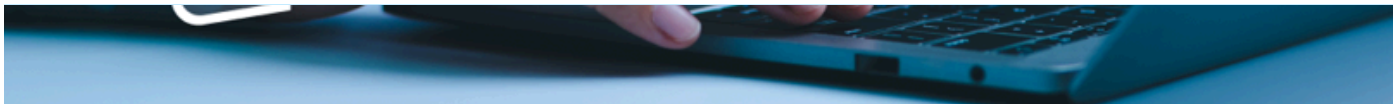
The NPRM proposed significant enhancements, such as:

- making all cybersecurity implementation specifications mandatory (eliminating the "addressable" guidance),
- requiring annual penetration testing,
- documenting asset inventories, and
- enhancing documentation.

The OCR requires the latter to demonstrate an organization's due diligence in complying with the Security Rule. The comment period closed on March 7, 2025, with no final rule issued under the current administration. Therefore, for now, organizations adhere to the current regulations.

As OCR audits intensify in 2025 and 2026, we will continue to see healthcare organizations entangled in investigations and legal proceedings with impacts that may include:

- Proliferation of Enforcement Investigations: With more than 400 active breach investigations as of August 2025 and audits expanding to 50 entities in the current cycle, covered entities and business associates will face prolonged scrutiny, on-site reviews, and potential civil lawsuits that could extend into 2027.



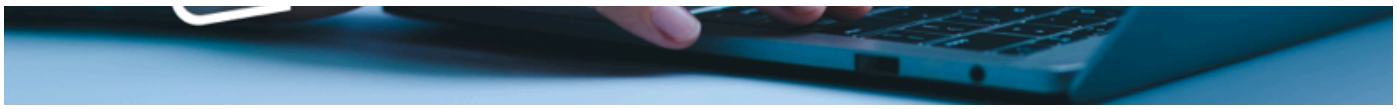
- Heightened Criminal Liability Risks: Repeat offenders of non-compliance uncovered by OCR audits could escalate to criminal charges under HIPAA's enforcement provisions, particularly for willful neglect, potentially exposing healthcare leaders to personal penalties and prison.
- Supply-Chain Litigation from Business Associates: Audits that reveal gaps in third-party oversight may spark indemnity claims and joint liability in breaches, as seen in the 2025 cases involving vendors such as Change Healthcare, which resulted in multi-million-dollar class-action suits.
- Rising Financial Penalties: As OCR continues to intensify its audits on Security Rule deficiencies, fines of up to $50,000 per violation can ensue with a $1.5 million annual cap, as demonstrated by the eight settlements from the Risk Analysis Initiative during the 2024-2025 timeframe.

The current statistics and OCR enforcement activities continue to highlight glaring gaps between industry compliance and the reality of the online threat environment. And while this may paint a bleak picture, healthcare organizations can fully turn their circumstances around by taking steps to fortify cybersecurity operations, improve compliance, and mitigate the impacts of escalating audits and potential fines.

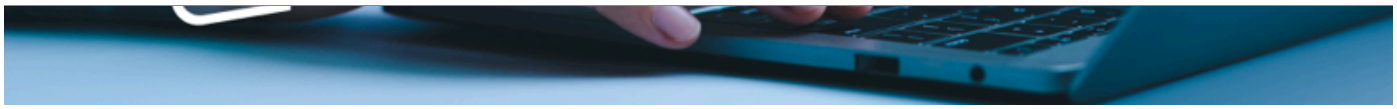
Prescription for Resiliency

So, what can you do now to bridge the compliance chasm and fortify cybersecurity operations? Consider the following steps:

CYBERSECURITY AWARENESS MONTH



1. Perform a thorough risk assessment. A recent SAI360 survey revealed that executives cite the need to perform risk assessments as a top priority; yet, only 8% of organizations conduct them — every two years at best — despite the annual mandate by 45 CFR § 164.308(a)(1). HHS offers a Security Risk Assessment Tool to help organizations identify and evaluate vulnerabilities in their systems, networks, and processes. However, independent third-party assessments are leading practices, as they tend to uncover more compliance gaps and enterprise risks that are often overlooked due to organizational biases or a lack of insight into trending issues and findings.
2. Train. Train. Train. Employees are the first line of defense against cyberattacks, and individuals often default to what they know or how they have been trained to respond. The more organizations equip their workforce with knowledge about the types of scams prevalent today (e.g., AI-generated email attacks), the better off the enterprise will be. While most organizations provide annual HIPAA training, nearly 21% of them skip knowledge testing, according to the HIPAA Journal's 2025 survey..
3. Conduct regular internal audits — at least annually. Nearly half (46%) of covered entities and business associates do not perform regular audits, a function that stress tests security policies, procedures, and management operations. Utilize the outcomes of internal audits to develop an action plan that mitigates risks and addresses compliance gaps, enabling organizations to stay ahead of evolving cyber threats. Appoint a HIPAA Privacy/Security Officer with decision-making authority; smaller entities can hire a Fractional Chief Privacy/HIPAA Security Officer to improve compliance and build resiliency without financially burdening their budget.

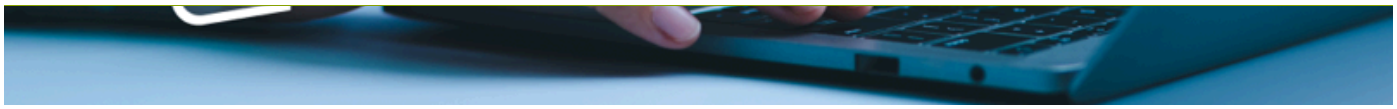


4. Leverage technology without compromising compliance. Organizations must implement encryption for ePHI data in transit and at rest (per 45 CFR § 164.312(e)), and should have multi-factor authentication (MFA) technology in place. The use of advanced anomaly detection and behavioral analytics tools to monitor network activities, prevent data loss, and possess endpoint detection and response (EDR) is a mainstay on most network systems in today's threat climate. Additionally, when working with third-party administrators and partners, conduct risk assessments to vet entities with whom you share risk and regularly monitor contractual agreements.
5. Prepare for the inevitable. Develop and test a comprehensive incident response plan based upon a structured cybersecurity framework (e.g., the NIST Cybersecurity Framework, ISO 27001). These frameworks outline specific controls and measures that cover, among other things, the detection, containment, eradication, and recovery phases, thereby minimizing downtime during a cyberattack or breach and demonstrating that a clear plan is in place. Finally, maintain tested backup and data recovery procedures that ensure constant offline, undisputable backups with regular testing to swiftly restore operations without reinfecting the network system.

Act Decisively

The wave of cybersecurity risks in healthcare is far from receding — ransomware groups continue to evolve, technology for nefarious activities advances, and regulations become tighter and enforced more strongly. By acting decisively on the recommendations above, organizations can transform uncertainty into resilience, protect patient data, avert audits, and insulate themselves from sanctions.

CYBERSECURITY AWARENESS MONTH



Your organization deserves better than being 'less than half' confident. Take effective measures to achieve full compliance and enhance cyber operations — start today. Contact us to discover how we can help you achieve your path to compliance and cybersecurity readiness.

Contact Us

Lynn Rohland
Gray Reed Advisory Principal
703.801.6075 | lrohland@grayreedadvisory.com

Vicky Fang
Gray Reed Advisory President
408.203.8778 | vfang@grayreedadvisory.com