Compliance Gaps That Put Healthcare Data at Risk

Cybersecurity
Progress. Protected.

Compliance Gaps That Put Healthcare Data at Risk

Despite all good-faith efforts to comply with HIPAA and other regulations that aim to protect personal health information, gaps in cybersecurity still happen to the best organizations. That's evidenced by the number of reported breaches, the results of cybersecurity audits reported by the HHS Office of Civil Rights (OCR), and the regulatory penalties and settlements reported.

The gaps are not necessarily caused by oversights, but rather practical limitations. Executives at resource-constrained health facilities were interviewed for a May 2025 report by a working group of more than 460 healthcare stakeholders including providers, manufacturers, payers and government agencies. A dominant theme shared among the interviewees, who serve small- and mid-sized communities, is that they know what they need to do to secure their organizations. They simply don't have the workforce capacity to do it.[1] While tackling regulatory compliance is itself a big undertaking, it has to be balanced against other priorities. **After all, the primary mission is patient care.** Striking the proper balance between investments in regulatory compliance and priorities that are seen as more directly related to the primary mission can be difficult.

Among the cybersecurity challenges that all healthcare organizations face, and that are especially felt by smaller organizations are:

Legacy systems

Devices that have outlived software support and no longer have updates and security patches require costly, inefficient workarounds and compensating controls to maintain functionality while operating securely. Some of these are regulated by the FDA, which further complicates the effort to secure them. If you're relying on legacy systems for some of your medical technology, you're not alone. **A 2023 survey found that 95% of hospitals were operating with end-of-life operating systems or software with known vulnerabilities.[2]**

Third-party vendor exposure

Reliance on unregulated third-party vendors for key services is a huge concern. While organizations are doing their due diligence in having business associate agreements in place as required by HIPAA and holding vendors accountable for breaches or vulnerabilities, nevertheless, in one study nearly one-fourth of healthcare organizations surveyed reported experiencing a ransomware attack caused by a third party.[3]

Cybersecurity staffing shortages

The shortage of cybersecurity professionals is keenly felt in the healthcare sector, as individuals who have the required skills often tend to choose other industries where the pay is better. Attracting and retaining talent is especially difficult for rural hospitals that have to make do with small teams who have other job responsibilities outside of cybersecurity or work part time.

Cyber insurance costs and requirements

Cybersecurity insurance premiums continue to rise and coverage is increasingly hard to get. Insurers mandate that organizations meet minimum security standards to qualify for coverage, and typically require regular audits to prove those standards are continuing to be met. These requirements can be difficult to meet for smaller organizations with restricted budgets and limited staff. When coverage can be obtained, it often comes with high deductibles, coverage limits and exclusions that means these organizations still have to accept some level of risk.

Regulatory complexity

With its requirement to execute a risk analysis and implementation steps that are a mix of required and addressable regulations, HIPAA has its own set of challenges. These were further extended by the requirements added by the HITECH Act, the HIPAA Omnibus Rule and other federal standards such as GINA. There are multiple sources of published guidance available at the federal level put out by various agencies but the recommendations often differ.

Moreover, focusing on federal regulations is no longer enough. Yet another layer of complexities come into play when you have to also consider the increasing amount of privacy legislation that has been and is being introduced at the state level. As of October 2025, the International Association of Privacy Professionals reports that 19 states have privacy laws in place that are intended to be comprehensive in terms of their scope, coverage, and rights offered to citizens. Another five states have bills active in the

[3] Healthcare and Public Health Sector Coordinating Council, Hospital Cyber Resiliency Initiative: Landscape Analysis. April 2023.

legislative process.[4] The state laws vary in terms of the organizations and data to which they apply, and the obligations of organizations that handle sensitive personal information. As a result, healthcare compliance professionals have to manage a web of regulations that overlap, with similarities and differences that are tricky to negotiate.

Common compliance gaps

The Healthcare and Public Health Sector Coordinating Council is a coalition of private-sector critical healthcare infrastructure entities organized to advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the healthcare sector. In May of 2023, the council published a report, *Considerations for Prioritized Recognized Cybersecurity Practices for the Healthcare Industry.* Amid the backdrop of increasing cyberthreats including ransomware and despite all efforts to comply with regulations, it provided this analysis of why compliance gaps continue to persist:

> ... the massive and increasing complexity of today's connected healthcare ecosystem gives rise to its own risks: of unanticipated and poorly understood interdependencies; of unknown inherited security weaknesses; of overreliance on vendor solutions; of systems that fail to adequately account for human factors related to cybersecurity controls; and of inconsistencies between software and equipment lifecycles, among others. As a result, we are adopting new technologies faster than we are updating security practices, therefore creating a growing gap between slowly developing security posture and rapidly evolving security threats.[5]

Among the most notable compliance gaps are:

Access control weaknesses

HIPAA requires covered entities to implement access controls on systems that maintain protected health information and to verify that a person or entity seeking access is the one claimed. Adoption of multi-factor authentication by U.S. hospitals has been fairly high at 90% but not applied consistently, with 84% of VPNs and 88% of email systems protected with MFA.[6] The lack of consistent adoption leaves vulnerabilities that can be exploited via single credentials that can be stolen or obtained via phishing attacks. Weak or insufficient access controls are one of the more common HIPAA violations. They have resulted in

[4] https://iapp.org/resources/article/us-state-privacy-legislation-tracker/#state-privacy-law-chart
[5] Healthcare and Public Health Sector Critical Infrastructure Security and Resilience Partnership, Considerations for Prioritized Recognized Cybersecurity Practices for the Health Industry. May 2023.
[6] Healthcare and Public Health Sector Coordinating Council, Hospital Cyber Resiliency Initiative: Landscape Analysis. April 2023.

penalties ranging from nearly $1 million in the case of access control failures alone to multiple millions of dollars when access control failures are found alongside other serious HIPAA violations.

Lack of encryption

HIPAA calls for encryption of ePHI as an addressable rather than an absolute requirement and to be implemented "whenever deemed appropriate". This seems to grant some leeway and put the judgement of whether to implement encryption or not up to the individual organization. However, while encryption is not technically mandatory, it cannot be ignored since addressable does not mean optional. Addressable means that if encryption is not applied, some other alternative, equally effective security measure must be put in place. The OCR has pointed to the failure to encrypt data in several million dollar and multi-million dollar penalties.

Lack of or insufficient monitoring

Under HIPAA, entities are required to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. Moreover, they are required to "identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes." Needless to say, smaller organizations without the budget to hire dedicated cybersecurity staff find these requirements difficult or impossible to meet.

Closing the most critical gaps

ESET PROTECT MDR directly addresses many of the gaps identified above.

Improved access control

In 2023, a public/private partnership released *Considerations for Prioritized Recognized Cybersecurity Practices for the Health Industry*. It identified MFA as one of the most impactful practices for mitigating risk, specifically pointing to its use for protecting all email access as well as remote access including VPNs, virtualized desktop environments and terminal

sessions.[7] ESET PROTECT MDR includes ESET Secure Authentication, which enforces login security with a second factor using an SMS or email message, push notification, third-party authentication client, biometric scan or hardware key.

Encryption of protected health information

Implementing encryption is addressable under the HIPAA Security Rule standards for access control and transmission security. HIPAA also grants safe harbor from the data breach notification rules if lost or stolen data is encrypted, and most U.S. states also exclude encrypted data under their data breach notification laws. ESET Full Disk Encryption, included in ESET PROTECT MDR, encrypts data stored on system disks, partitions or entire devices using AES-256 encryption.

Protection for legacy systems

Many healthcare organizations have to rely on devices built on older hardware platforms and OS's (such as Windows 7, XP or others) that are past end-of-life and no longer have security patches and upgrades available. ESET continues to track the CVEs for legacy systems and develops detection capabilities for threats that target those vulnerabilities.

Qualification for cyberinsurance coverage

As underwriters enforce tighter requirements for security as a condition for granting coverage or setting premiums, increasingly they look for MDR to be in place. ESET PROTECT MDR meets this requirement, depending on the specific provisions of the insurer. Moreover, ESET has already prequalified its MDR service with select cyber insurance brokers to make the approval process faster and easier.

Continuous monitoring

The HIPAA security incident procedures standard requires the covered entity to identify and respond to security incidents, mitigate harmful effects and security incidents, and document incidents and their outcomes. The ESET MDR service allows resource-constrained healthcare organizations to meet this required standard. In addition, having the ESET PROTECT Platform in place allows organizations to meet several other standards under the HIPAA Security.

[7] Healthcare and Public Health Sector Critical Infrastructure Security and Resilience Partnership, Considerations for Prioritized Recognized Cybersecurity Practices for the Health Industry. May 2023.

Addressing the gaps with ESET PROTECT MDR

ESET PROTECT MDR is a managed detection and response service that is bundled with ESET's comprehensive endpoint protection. Its combination of security technologies including artificial intelligence coupled with human intelligence addresses compliance gaps both identified and unknown. With ESET Endpoint Security installed on the computers, laptops, and servers in your environment, ESET's team of security analysts are able to monitor the traffic passing through your endpoints. Artificial intelligence-driven automated detection capabilities with continuous oversight by ESET security analysts detects suspicious behavior by threat actors exploiting gaps in security. While according to Ponemon, the healthcare industry's average time to identify and contain a data breach is 279 days, ESET PROTECT MDR is able to block, contain and remediate threats with a mean response time of six minutes..

Protecting healthcare organizations with six-minute mean time to respond.

The ESET MDR service is able to detect and respond instantly and effectively stop an attack in its tracks. It harnesses ESET's 30 years of deep human cybersecurity experience and expertise and applies it at scale through cutting-edge artificial intelligence to cost-effectively protect your healthcare organization. A combination of automation, human intelligence and artificial intelligence all work together to eradicate the simplest threats automatically and allow security analysts to focus on what really matters.

The ESET MDR service has extensive reporting capabilities that your internal security teams have access to. It also generates reports that are appropriate for non-technical audiences so you can demonstrate to and assure executives that your organization is protected. This reporting capability supports your efforts to document your compliance, and to respond to security audits.

If you are a small or mid-sized healthcare organization, ESET MDR gives you a comprehensive, holistic solution to your compliance challenges, 24/7.

ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network, led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

Cybersecurity
Progress. Protected.