Briefings on HIPAA

Lessons learned from latest high-dollar Security Rule settlement

by Dom Nicastro

The Office for Civil Rights (OCR) has reached a $950,000 settlement with Heritage Valley Health System, Inc. for potential violations of the HIPAA Security Rule, following an OCR investigation after the health system experienced a ransomware attack in 2017.

The investigation revealed several potential violations, including failures to:

- Conduct a compliant risk analysis to identify risks and vulnerabilities to electronic protected health information (ePHI)
- Implement a contingency plan to address emergencies like ransomware attacks
- Establish policies and procedures to prevent unauthorized access to ePHI

As part of the resolution, Heritage Valley will pay a $950,000 settlement and adhere to an OCR corrective action plan for three years. The health system will take a number of steps to resolve potential violations of the HIPAA Security Rule and protect its ePHI, including:

- Conducting an accurate and thorough risk analysis to determine potential vulnerabilities related to the confidentiality, integrity, and availability of ePHI
- Implementing a risk management plan to mitigate the vulnerabilities identified in its risk analysis
- Reviewing and developing its written policies and procedures to comply with the HIPAA rules
- Training its workforce on HIPAA's policies and procedures

OCR notes it has seen a 264% increase in reports of large ransomware breaches since 2018. It recommends healthcare providers, health plans, clearinghouses, and HIPAA-covered business associates take the following steps to mitigate and/or prevent cyberthreats:

- Review all vendor and contractor relationships to ensure business associate agreements (BAA) are in place as appropriate and address breach/security incident obligations
- Integrate risk analysis and risk management into business processes, conducted regularly and when new technologies and business operations are planned
- Ensure audit controls are in place to record and examine information system activity
- Implement regular review of information system activity
- Utilize multifactor authentication (MFA) to ensure only authorized users are accessing ePHI
- Encrypt to guard against unauthorized access to ePHI
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to the organization and to workforce members' job responsibilities on a regular basis; reinforce the workforce's critical role in protecting privacy and security

Risk analysis and management

Maha Shahid, content specialist at CureMD and a provider specializing in IT healthcare solutions, says conducting a comprehensive risk analysis involves using standardized frameworks like NIST's Risk Management Framework or ISO 27001. This process includes identifying assets containing ePHI, assessing potential threats and vulnerabilities, and implementing appropriate security measures.

Ensuring compliance with the HIPAA Security Rule involves regular use of resources like the HIPAA Security Risk Assessment (SRA) Tool.

"Risk management plans should be updated regularly, particularly after significant organizational changes or security incidents," he says. "Effective vulnerability management involves patch management, strict access controls, encryption, and continuous monitoring to detect and respond to threats in real time."

Organizations should conduct a comprehensive risk analysis annually, with quarterly updates to address any changes. Any significant organizational changes, new technologies, regulatory updates, security incidents, vendor changes, market shifts, or internal audit findings should trigger an immediate review.

Common pitfalls include failing to comprehensively identify potential risks, not keeping the assessment up to date with

changes in the organization, and poorly documenting the assessment process, Shahid says. “Additionally, involving cross-functional teams and leveraging external expertise can enhance the thoroughness and accuracy of the assessment.”

Encryption protects sensitive patient data during transmission, preventing breaches even if intercepted by unauthorized parties. Similarly, strict access controls ensure that only authorized personnel can access critical systems and data, significantly reducing the risk of internal threats. For example, MFA has prevented unauthorized access attempts, safeguarding confidential patient information.

“Organizations can balance robust access controls with user convenience by implementing adaptive [MFA] solutions that consider the context of access requests, such as location, device, and user behavior,” Shahid says. “Using single sign-on (SSO) combined with MFA reduces the number of times users need to authenticate while maintaining security.”

Contingency planning

Best practices for developing contingency plans include conducting thorough risk assessments, performing business impact analyses, and establishing robust data backup procedures.

A business impact analysis should identify critical business functions and processes, as well as assess the potential impact of disruptions on these areas, according to Shahid. It should also outline recovery time objectives, recovery point objectives, and resource requirements to ensure comprehensive preparedness and effective response, he adds.

“A contingency plan should consist of disaster recovery protocols and clear communication strategies,” Shahid says. “Regular simulations and drills are essential to test and refine the plan, ensuring preparedness for emergencies like ransomware attacks.”

Organizations should conduct simulations and drills at least twice a year to ensure readiness for potential incidents. Best practices include involving all relevant departments, using realistic scenarios, conducting both announced and unannounced drills, and thoroughly reviewing the outcomes to identify areas for improvement.

Integrating lessons learned from actual incidents and continuously updating the drill scenarios can enhance overall preparedness. For example, Shahid recalls a significant ransomware attack in which his team’s past experience and robust training greatly assisted in executing the team’s contingency plan (i.e., isolating affected systems to prevent further spread, communicating with stakeholders, and initiating data recovery from secure backups).

“Our incident response team worked around the clock,” he says. “Within 48 hours, we had restored critical operations without data loss. The comprehensive training and simulation exercise we had conducted prior to the incident played a crucial role.”

Policies and procedures

Organizations should adopt a proactive approach to updating their policies and procedures and stay ahead of regulatory changes and emerging threats. At minimum, they should schedule annual reviews of policies and procedures, updating them as necessary to reflect shifts in regulations, according to Shahid.

The work of keeping up with regulations includes establishing a dedicated compliance team responsible for continuously monitoring regulatory updates and industry trends. Reviewing and revising policies and procedures, incorporating feedback from audits and risk assessments, and ensuring clear communication and training for all employees are essential to keep teams on the cutting edge of safety.

“Leveraging technology for real-time monitoring and automating policy management can also enhance the efficiency and effectiveness of this process,” Shahid says.

Vendor and contractor relationships

Managing vendor and contractor relationships requires thorough due diligence, including evaluations based on security certifications and adherence to industry standards.

“Regular audits and site visits ensure ongoing compliance,” Shahid says. “[BAAs] must clearly outline breach notification procedures and security incident responsibilities, with regular reviews and updates to reflect current best practices and regulatory requirements.”

To ensure thorough breach notification and security incident management, a BAA should include several key elements:

- Detailed definitions of what constitutes a breach and a security incident
- Clear timelines for notification
- Specific procedures for reporting and managing these events
- Both parties’ responsibilities for investigating and mitigating breaches, maintaining compliance with relevant

regulations, and conducting regular risk assessments

For Shahid’s own firm, regular audits and site visits have proven invaluable in ensuring vendor compliance. “For instance, during a [recent] routine audit and site visit to a key vendor's facility, we identified gaps in their data encryption practices and access control measures,” he says. “This discovery led to immediate corrective actions, including enhanced encryption protocols and stricter access controls, significantly bolstering their security posture. Continuous follow-up audits and visits ensured these measures were sustained, ultimately protecting our client’s sensitive data and maintaining regulatory compliance.”

When evaluating potential vendors or contractors for security compliance, organizations should consider several key criteria. These include the vendor's adherence to industry standards and regulations, their track record of handling security incidents, and the robustness of their security infrastructure and protocols.

Some of the most effective tools Shahid uses for real-time threat detection include:

- Platform offerings from Splunk, which provides robust analytics and monitoring capabilities
- Palo Alto Networks' Cortex XDR™, popular for its advanced threat detection and response features
- CrowdStrike Falcon®, offering comprehensive endpoint protection and rapid threat detection
- IBM QRadar®, which excels in security information and event management (SIEM)
- Microsoft Defender for Endpoint, which provides integrated threat protection across the enterprise
- Incident response and audit controls

Developing a robust incident response process includes creating a detailed incident response plan that outlines roles, responsibilities, and procedures for managing security incidents.

Using automated tools for monitoring and analyzing system activity logs, scheduling regular audits, and enforcing robust access controls is also key to effective incident response. Implementing MFA further secures access to ePHI, ensuring comprehensive protection.

“I recommend using Splunk and IBM QRadar for monitoring and analyzing system activity logs,” he says. “Both tools offer robust alerting, reporting, and integration features, making them essential for maintaining a secure and compliant IT environment. Splunk excels in its ability to handle large volumes of data, providing real-time insights and powerful search capabilities to identify and mitigate potential threats quickly. IBM QRadar is highly effective because of its advanced security analytics and correlation capabilities, which help in identifying sophisticated security incidents.”

Training never ends

Comprehensive training programs for new employees and ongoing education sessions are crucial to maintaining compliance. Opt for methods such as quizzes and practical exercises to better promote understanding and adherence to policies, according to Shahid.

“Interactive training methods that have proven effective in promoting compliance include scenario-based learning, where employees engage in simulations of real-life situations they might encounter,” he says. “Role-playing exercises allow staff to practice responding to compliance issues, while gamification elements, such as quizzes and rewards, make learning engaging and reinforce key concepts.”