Briefings on HIPAA

Strengthening cyber defenses: What hospitals can learn from ransomware breach

by Dom Nicastro

We continue to explore the findings of OCR's $950,000 settlement with Heritage Valley Health System over potential violations of the HIPAA Security Rule. This settlement comes in the wake of a ransomware attack, highlighting the growing threat of cyberattacks in the healthcare sector and underscoring the critical need for robust cybersecurity measures.

Heritage Valley, which operates in Pennsylvania, Ohio, and West Virginia, faced a ransomware attack that exposed vulnerabilities in its electronic protected health information (ePHI) systems. OCR's investigation into the incident revealed several potential violations of the HIPAA Security Rule, including:

- **Failure to conduct a compliant risk analysis:** Heritage Valley did not perform an adequate risk analysis to identify potential risks and vulnerabilities to ePHI in its systems.
- **Lack of a contingency plan:** The organization failed to implement a contingency plan to respond to emergencies, such as ransomware attacks, that could damage systems containing ePHI.
- **Insufficient access controls:** Heritage Valley's policies and procedures did not adequately ensure that only authorized users had access to ePHI.

We caught up with **Dan Ongaro,** senior associate for global regulatory at law firm Hogan Lovells, for a Q&A on these security topics.

Risk analysis and management

Q: How can HIPAA security leaders conduct a comprehensive risk analysis to identify vulnerabilities in their systems?

Ongaro: A key aspect of conducting a comprehensive risk analysis that satisfies HHS OCR's expectations is understanding the scope of ePHI data and applicable assets. Just as important can be confirming the scope of data and systems that are not subject to HIPAA, to establish clear boundaries for purposes of the risk analysis.

From this initial inventory, organizations can tailor the risk analysis to focus on the organization's specific environment and the potential "attack surface."

For example, the balance of certain risks are different for an organization that employs mostly on-premise systems than one that operates mostly in the cloud. HHS OCR has been clear that the Security Rule does not prescribe a specific risk analysis methodology, but assessments need to be accurate and thorough. A great starting point is referencing NIST SP 800-30.

A common issue HHS OCR has noted is when organizations submit a compliance or gap assessment as the risk analysis. Such assessments typically do not include a discussion of potential threats and vulnerabilities, but instead review security safeguards against a given framework/standard (whether the HIPAA Security Rule, ISO, or NIST). It can still be useful to incorporate such assessments into a risk analysis, to help confirm the status of current security safeguards and provide context for residual risk scoring.

Q: What strategies can be used to regularly update risk management plans, and what events should trigger these updates?

Ongaro: The Security Rule does not specify how frequently to perform a risk analysis or updates to risk management plans, but a truly integrated risk analysis likely is updated as new technologies and business operations are planned, as well as when new threats emerge.

This does not mean redoing the entire process each time from scratch, but revisiting if the nature of threats has changed or there are key updates to an inventory (e.g., because of an acquisition or new operating segment).

Similarly, it is often helpful to integrate periodic updates to risk management plans consistent with broader governance activities, such as quarterly oversight or steering committee meetings, or executive leadership or board committee briefings.

Q: What steps can be taken to effectively address vulnerabilities identified in a risk analysis?

Ongaro: After the risk analysis is complete, the results can be a direct input to an organization's risk management process to assist the organization in developing corrective actions or security enhancements to support meeting the organization's risk tolerance.

Strategies we have seen work well for addressing vulnerabilities are when the organization breaks down action plans into concrete milestones with clear resources assigned and integrates large-scale plans into the organization's broader IT road map. It is important to have an open and honest conversation about whether the identified vulnerability actually presents a level of risk requiring further action, as well as which risk management strategy—including avoidance or transfer—may be appropriate in the circumstances; not every identified vulnerability or risk necessarily merits remediation.

Contingency planning

Q: What are the best practices for developing a contingency plan to respond to emergencies like ransomware attacks?

Ongaro: For a contingency plan to be particularly effective, the plan should consider dependencies, including those from third-party systems that would be critical to the restoration of services, and be grounded in a clear understanding of relative criticality.

Further, because threat actors often target backups in an attempt to inhibit restoration of operations, the contingency plan and related processes should account for this tactic and consider security controls such as dual authentication and immutable, encrypted backups to decrease the risks of a ransomware attack.

Q: What key components should be included in a contingency plan to ensure effectiveness during an actual attack?

Ongaro: NIST SP 800-34 and other guidance detail key components to include in a contingency plan and related documents.

However, for many organizations, even if their contingency plans address the components, they are often covered at a superficial or too abstract of a level to be particularly effective in practice. Organizations do not always go through the process to fully assess dependencies/prerequisites and erroneously rely on assumptions that other aspects are fully functional and available.

It is also critical to confirm that there is a documented plan in place to address any key processes that would require manual alternative processes in the event of a prolonged outage.

Q: How can lessons learned from past incidents be used to improve existing contingency plans?

Ongaro: One trend we are seeing is greater integration of incident response plans and contingency plans, including for testing exercises. Rather than viewing each document in a vacuum (often with separate owners) and viewing a contingency plan as purely operational, we are seeing greater consideration of data security as part of contingency plans and vice versa.

Tabletop exercises can home in on the restoration and recovery components of incident scenarios, informed by the organization's past incidents and any "near misses" or pain points. Further, technical testing exercises, including actual restoration from backups, often proactively identify shortcomings with contingency plans.

Policies and procedures

Q: How can HIPAA security leaders ensure that their policies and procedures are fully compliant with HIPAA Security Rule requirements?

Ongaro: Going beyond the HIPAA Security Rule's high-level text, organizations are well advised to look to guidance HHS OCR has published, in particular the audit protocols, as HHS OCR has announced plans for the next round of these audits.

In addition, HHS OCR has developed crosswalks to security guidance such as NIST CSF and associated NIST publications, as well as authored newsletters and other guidance that goes in more depth on various key topics.

Organizations can also refer to recent enforcement actions by HHS OCR to better understand common issues identified, to make certain their policies and procedures address these alleged deficiencies.

Q: What methods can be employed to review and update policies and procedures on a regular basis?

Ongaro: Many companies have transitioned to a document management system that sets up automated alerts for documents to be reviewed after an established period of time (e.g., annually) and to capture evidence of the review and approval process. There are other project management tools smaller companies can use to achieve the same goal.

Beyond a prescribed periodic review, having defined stakeholders in charge of a document or portions of a document helps encourage accountability for the update to accurately capture changes to the system and broader environment.

It also can be helpful to review any policy exceptions granted since the last policy review/approval as part of periodic reviews, to help inform whether changes to policies or procedures may be warranted as well as to identify patterns suggesting policies are increasing business friction or compliance risk.

Q: How can organizations effectively train their workforce on these policies and procedures to ensure compliance?

Ongaro: Training continues to become more interactive, and we have seen more clients shift to ongoing reminder exercises and gamification to avoid training being seen as merely an annual check-the-box exercise.

As part of training, we also have seen more companies shift to incorporate actual policies (or at least reinforce where workforce members can access these policies) so that when the time comes and an employee wishes to clarify certain information, the employees know where to turn.

Periodic reminders that use real-world threats, such as showcasing a recent social engineering campaign, are an excellent opportunity to reinforce security expectations and drive compliance—while reminding workforce of relevant policies and procedures to follow.

Vendor and contractor relationships

Q: What approaches can HIPAA security leaders use to manage relationships with vendors and contractors to ensure compliance with HIPAA security requirements?

Ongaro: Relationship management should begin with a risk assessment of the vendor or contractor. Not all vendors and contractors present the same level of risk to the organization because of the corresponding level of data or system access. The business associate agreements and related terms and conditions can be tailored based on the risk level.

Further, higher-risk vendors and contractors may be subject to greater ongoing monitoring or other requirements to confirm HIPAA security compliance.

Also, it is very important to reassess the level of risk over time, as vendor relationships may change or grow. For example, one pitfall we've seen in the past is a vendor being approved for an initial pilot or nonproduction data handling, only to end up years later with that same vendor interacting with the organization's most sensitive PHI repositories.

Q: What criteria should be used to assess the security practices of vendors and contractors?

Ongaro: We still see questionnaires used as the primary method of up-front diligence. The questionnaires help inform risk-based decisions and associated contractual terms and conditions regarding security. It can be helpful to accept well-established security certifications and audits as a basis to streamline such questionnaires—akin to allowing workforce to take streamlined training if they "test out" of certain modules.

We also have seen greater adoption of threat intelligence tools by sophisticated companies to conduct ongoing monitoring.

Incident response and audit controls

Q: How can HIPAA security leaders develop a robust incident response process to handle ransomware attacks?

Ongaro: For ransomware in particular, having the incident response process intertwined with contingency planning, including coordinated testing and training exercises, is key. Given the unique nature of ransomware, we also commonly see clients develop a separate "playbook" as an appendix to the incident response plan that considers the various decision points and nuances with ransomware.

Effective ransomware response plans are invariably multistakeholder concepts, drawing on input and decision-making from executive leadership, legal, privacy, compliance, and other functions far beyond IT/privacy/security.

Further, to be realistic, training for ransomware should include participants from senior leadership, who would be the ultimate decision-makers in a real ransomware incident.

Q: What are the best practices for utilizing audit controls to monitor and examine information system activity?

Ongaro: We operate in an era where organizations risk being overwhelmed by the sheer volume of logs and information available for review, as well as corresponding growth in the number of alerts. We continue to see greater adoption of centralization/aggregation of audit logs into increasingly sophisticated SIEM [security and information event management] tools to correlate the various audit logs and detect anomalous system activity.

Further, it's important that alert tuning is an ongoing exercise so that "noise" is minimized to decrease the likelihood of alert fatigue. Having alerts that are not resolved may lead to greater regulator scrutiny than if the organization never knew of the problem to begin with.

Organizations often engage a third-party service provider, such as a managed security service provider, to help manage the triage and initial review of such logs or otherwise confirm that there is clear assigned responsibility within the organization for review, prioritization, and resolution of such alerts.