Ransomware and HIPAA – A Primer

by J. Ryan Williams, Esq. // Co-Chair of the Health Care Practice Group, Brouse McDowell

Your healthcare provider organization recently suffered a ransomware attack that involved its electronic medical records system (EMR). You have been scrambling to regain access to the EMR (and have likely paid the ransom to expedite the restoration of the EMR). Now that you have moved past the initial disruption caused by the ransomware attack, you turn your attention to reviewing and assessing the situation. You do not need to look far for guidance – the Health Insurance Portability and Accountability Act (HIPAA) security and breach notice rule should play a significant role in your review and assessment.

The Office of Civil Rights (OCR), the federal oversight agency charged with enforcing HIPAA, takes the position that a ransomware attack rises to the level of a "security incident" under the HIPAA security rule. Thus, any review or assessment of a ransomware attack should involve the organization's security incident policy.

A HIPAA compliant security incident policy should require a thorough analysis to determine: (1) the scope of the incident to identify what networks, systems, or applications are affected; (2) the origination of the incident (who/what/where/when); (3) whether the incident is finished, is ongoing or has propagated additional incidents throughout the environment; and (4) how the incident occurred (e.g., tools and attack methods used, vulnerabilities exploited). OCR suggests initiating this analysis as soon as the ransomware attack is discovered. However, in the chaos of the moment, and given that an attack can render entire systems, including EMRs, completely inaccessible, organizations typically put all efforts into regaining access using just about any means necessary.

Nevertheless, this analysis is the foundation of the organization's overall review and assessment of the situation. For example, this analysis will help the organization conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the organization has any regulatory, contractual or other obligations as a result of the incident. The organization must also incorporate this analysis into the overall security management process of the organization to improve incident response effectiveness for future security incidents. At a minimum, the organization should review this analysis in connection with future security risk assessments performed in compliance with the HIPAA security rule.

In addition to the security incident analysis, the organization must determine whether the ransomware attack constitutes a breach of protected health information (PHI). Since the HIPAA breach notice rule applies to the breach of unsecured PHI, which means PHI that has not been properly encrypted at all stages, the first step in any breach analysis is to assess the encryption status of the affected PHI. Simply determining that the PHI was encrypted is not enough. OCR cautions that many ransomware attacks appear as authentic user access and thus may override encryption technologies. If this is the case and the PHI is decrypted as part of an otherwise authenticated access and then re-encrypted by the ransomware, a breach may have occurred.

If the ransomware attack does involve unsecured PHI, the organization must then conduct an assessment under its HIPAA breach notice policy to determine whether there is a low probability that the PHI has been compromised by the ransomware attack. A low probability of compromise does not require notice to patients and others. An organization's HIPAA breach notice policy should set forth the basic factors used to conduct the breach assessment.

Organizations that have never experienced a ransomware attack are becoming the exception, not the norm. These attacks and other similar schemes are becoming commonplace. Organizations that have robust HIPAA security policies in place are in the best position to swiftly address ransomware attacks in real time and thus minimize any consequences.

J. Ryan Williams represents health care providers in all aspects of healthcare transactions and related regulatory matters, including negotiation, due diligence, structure, and consummation of acquisitions, divestitures, leases, management arrangements, and joint venture transactions; regulatory compliance matters; licensure, certification, and reimbursement issues; fraud and abuse guidance; and health information technology projects.