THE
NATIONAL LAW REVIEW

Guidance on Ransomware Attacks under HIPAA and State Data Breach Notification Laws

McDermott Will & Emery

Article By
Angela M. Stockbridge
Michael G. Morgan
McDermott Will & Emery
On the Subject

- Communications, Media & Internet
- Health Law & Managed Care

- All Federal

Monday, August 8, 2016

On July 28, 2016, ***US Department of Health and Human Services (HHS)*** issued guidance (guidance) under the ***Health Insurance Portability and Accountability Act (HIPAA)*** on what covered entities and business associates can do to prevent and recover from ransomware attacks. Ransomware attacks can also trigger concerns under state data breach notification laws.

What Is Ransomware?

Ransomware is a type of malware (malicious software). It is deployed through devices and systems through spam, phishing messages, websites and email attachments, or it can be directly installed by an attacker who has hacked into a system. In many instances, when a user clicks on the malicious link or opens the attachment, it infects the user's data. Ransomware attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware. After the user's data is encrypted, the ransomware attacker directs the user to pay a ransom in order to receive a decryption key. However, the attacker may also deploy ransomware that destroys or impermissibly transfers information from an information system to a remote location controlled by the attacker. Paying the ransom may result in the attacker providing the key necessary

needed to decrypt the information, but it is not guaranteed. In 2016, at least four hospitals have reported attacks by ransomware, but additional attacks are believed to go unreported.

HIPAA Security Rule and Best Practices

The HIPAA Security Rule requires covered entities and business associates to implement security measures. It also requires covered entities and business associates to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic protected health information (ePHI) the entities create, receive, maintain or transmit and to implement security measures sufficient to reduce those identified risks and vulnerabilities to a reasonable and appropriate level. The HIPAA Security Rule establishes a floor for the security of ePHI, although additional and/or more stringent security measures are certainly permissible and may be required under state law. Compliance with HIPAA's existing requirements provides covered entities and business associates with guidance on how to prevent and address breaches that compromise protected health information. The new HIPAA guidance specific to ransomware reinforces how the existing requirements can help an entity protect sensitive information.

HHS has suggested that covered entities and business associates frequently back up their documents because ransomware denies access to the covered entity's and business associate's data. Maintaining frequent backups and ensuring the ability to recover data from a separate backup source is crucial to recovering from a ransomware attack. Test restorations should be periodically conducted to verify the integrity of backed-up data and provide confidence in an organization's data restoration capabilities. Because some ransomware variants have been known to remove or otherwise disrupt online backups, entities should consider maintaining backups offline and inaccessible from their networks.

Covered entities and business associates should also install malicious software protections and educate its workforce members on data security practices that can reduce the risk of ransomware, including how to detect malware-type emails, the importance of avoiding suspicious websites and complying with sound password policies.

Lastly, each covered entity or business associate should ensure that its incident response plan addresses ransomware incidents. Many entities have crafted their policies and incident response plans to focus on other more typical daily personal information risks, such as the lost laptop or personal device. A ransomware event should expressly trigger the activities required by the incident response plan, including the requirement to activate the response team, initiate the required investigation, identify appropriate remediation, determine legal and regulatory notification obligations, and conduct post-event review.

Indications of a Ransomware Attack

Indicators of a ransomware attack could include:

- The receipt of an email from an attacker advising that files have been encrypted and demanding a ransom in exchange for the decryption key
- A user's realization that a link that was clicked on, a file attachment opened or a website visited may have been malicious in nature
- An increase in activity in the central processing unit (CPU) of a computer and disk activity for no apparent reason (due to the ransomware searching for, encrypting and removing data files)
- An inability to access certain files as the ransomware encrypts, deletes and renames and/or relocates data
- Detection of suspicious network communications between the ransomware and the attackers' command and control server(s) (this would most likely be detected by IT personnel via an intrusion detection or similar solution)

What to Do if Subject to a Ransomware Attack?

A covered entity or business associate that is subject to a ransomware attack may find it necessary to activate its contingency or business continuity plans. Once the contingency or business continuity plan is activated, an entity will be able to continue its day-to-day business operations while continuing to respond to, and recover from, a ransomware attack. The entity's robust security incident procedures for responding to a ransomware attack should include the following processes to:

- Activate the entity's incident response plan and follow its requirements;
- Notify the entity's cyber liability insurer as soon as enough information is available to indicate a possible ransomware attack and within any time period required under the applicable policy;
- Detect and conduct an analysis of the ransomware, determining the scope of the incident and identifying what networks, systems or applications are affected;
- Determine the origin of the incident (who/what/where/when), including how the incident occurred (*e.g.,* tools and attack methods used, vulnerabilities exploited);
- Determine whether the incident is finished, is ongoing or has propagated additional incidents throughout the environment;
- Contain and eradicate the ransomware and mitigate or remediate vulnerabilities that permitted the ransomware attack and propagation;
- Recover from the ransomware attack by restoring data lost during the attack and returning to "business-as-usual" operations; and
- Conduct post-incident activities, which could include a deeper analysis of the evidence to determine if the entity has any regulatory, contractual or other obligations as a result of the incident (such as providing notification of a

breach of protected health information), and incorporating any lessons learned into the overall security management process of the entity to improve incident response effectiveness for future security incidents.

Additionally, it is recommended that an entity infected with ransomware consult, early on, with legal counsel who can assist with reporting the incident to the extent it is a criminal matter to law enforcement. Counsel frequently have ongoing contacts within the cybercrime units of the Federal Bureau of Investigation (FBI) or the United States Secret Service that may deploy appropriate resources to address the matter and to supply helpful information. These agencies work with federal, state, local and international partners to pursue cyber criminals globally and assist victims of cybercrime. Counsel can advise on the type of information appropriate to disclose to law enforcement, while taking steps to establish and maintain the attorney-client privilege and, if appropriate, the attorney work product protection. Counsel also can assist in preparing communications (*e.g.,* mandatory notifications and reports to senior executives and boards), advise on potential legal exposure from the incident and provide representation in connection with government inquiries or litigation.

If Ransomware Infects a Covered Entity's or a Business Associate's Computer System, Is It a *Per Se* HIPAA Breach?

Not necessarily. Whether or not the presence of ransomware would be a breach under the HIPAA Privacy Rule or HIPAA Security Rule (the HIPAA Rules) is a fact-specific determination. A breach under the HIPAA Rules is defined as, "...the acquisition, access, use or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." A covered entity or business associate should, however, perform a risk assessment after experiencing a ransomware incident to determine if a reportable breach has occurred and to determine the appropriate mitigating action.

If the ePHI was encrypted prior to the incident in accordance with the HHS guidance, there may not be a breach if the encryption that was in place rendered the affected PHI unreadable, unusable and indecipherable to the unauthorized person or people. If, however, the ePHI is encrypted by the ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (*i.e.,* unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule.

Thus, in order to determine if the information was acquired and accessed in the incident, additional analysis will be required. Unless the covered entity or business associate can demonstrate that there is a "[l]ow probability that the PHI has been compromised," based on the factors set forth in the HIPAA breach notification rule, a breach of PHI is presumed to have occurred. If a breach has occurred, the entity must comply with the applicable breach notification provisions under HIPAA and, if applicable, state law.

Does a Ransomware Event Trigger State Data Breach Notification Obligations?

Possibly. In a majority of states, data breach notification requirements are triggered

when there is both “unauthorized access” to and “acquisition” of personally identifiable information. Whether a ransomware event meets the access and acquisition elements of these statutes is, as in the HIPAA analysis, a fact-specific determination. If, for example, the hackers were able to move the personally identifiable information from the entity’s network to their own, it is clear that the hackers achieved unauthorized access to and acquisition of the information. State data breach notification laws pertaining to the affected individuals would need to be analyzed and factored into the entity’s overall notification requirements.

Ransomware though is usually designed to extort money from victim entities rather than steal personally identifiable information. If the forensics team can present credible evidence that no personally identifiable information was *acquired* by the hackers, then these obligations may not be triggered. The forensics team, consistent with the incident response team requirements, should document findings that support a defensible decision under these statutes, in case of a subsequent regulatory investigation or litigation, not to notify affected individuals.

In a minority of states, the data breach notification requirements are triggered when there is simply “unauthorized access” to personally identifiable information. This lower standard may mean that the entity must notify its customers of a data breach even when no personally identifiable information is acquired by a hacker. Entities that maintain personally identifiable information of residents of Connecticut, New Jersey and Puerto Rico, for example, may find themselves in the unfortunate position of having to provide data breach notifications even when the information is not acquired by a hacker.

Finally, if the entity is providing services to a business customer, it will need to determine whether it is obligated to notify the business customer (as owner of the affected personal information) of the ransomware attack, taking into account state data breach notification requirements, contractual obligations to notify the business customer and the overall value of the commercial relationship