Responding to a Ransomware Attack

Guidance from HHS on a healthcare provider's obligations under HIPAA

By Kimberly T. Boike, Esq. and Ryan Haas, Esq.

CYBERATTACKS directed at healthcare providers have become increasingly common. In fact, in issuing its ransomware guidance, the U.S. Department of Health and Human Services (HHS) specifically noted that in 2016 there were about 4,000 daily ransomware attacks, which represents a 300% increase over the 1,000 ransomware attacks reported in 2015. Part of the reason that attacks have become so common in the healthcare community is that medical records are worth more money on the dark web than credit card information or social security numbers. And no healthcare provider is immune from the risks of such attacks. Gone are the days when hackers focused on large sophisticated healthcare systems. Now, providers of all sizes across the continuum of care are targeted.

"Medical records are worth more money on the dark web than credit card information or social security numbers."

What is Ransomware?

Ransomware is a type of malicious software that is used by hackers to infiltrate and encrypt a healthcare provider's data. It is often delivered to a provider's system when a person on the healthcare provider's network clicks on a link within an email sent by a hacker, which downloads the ransomware to the provider's system. These emails have become increasingly sophisticated, making it difficult for individuals receiving the emails to identify them as suspicious. Once the ransomware has been downloaded, the provider's system becomes encrypted and the provider is unable to access its data, which may include its electronic medical records. The ransomware will then specify that if the healthcare provider desires to obtain the decryption key in order to regain access to its system, the provider must pay the hacker a ransom in cryptocurrency.

Healthcare Provider Obligations

Under the HHS guidance, if a healthcare provider's system is infected with ransomware, a security incident has occurred under the HIPAA Security Rule. A security incident is "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." Therefore, the provider must follow its security response and reporting procedures under HIPAA when an attack occurs. According to HHS, a provider's incident response activities should include determining the scope of the issue, how the issue originated, whether the issue is ongoing and how the issue occurred. Once these determinations have are made, the healthcare provider must engage in a more thorough analysis to determine if the security incident resulted in a breach under HIPAA.

A Breach Under HIPAA?

HIPAA defines a breach as the acquisition, access, use or disclosure of protected health information in a manner not permitted by HIPAA that compromises the security or privacy of the protected health information. This acquisition, access, use or disclosure is presumed to be a breach unless the healthcare provider demonstrates there is a low probability the protected health information has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the protected health information or to whom the disclosure was made.
- Whether the protected health information was actually acquired or viewed.
- The extent to which the risk to the protected health information has been mitigated.

In the HHS guidance, the agency takes the position that when electronic protected health information is encrypted in connection with a ransomware attack, then a breach has occurred. HHS' reasoning is that in a ransomware attack, the hacker's taking possession or control of protected information is a disclosure not permitted under HIPAA.

Unless a provider can show there was a low probability the protected health information was compromised, the healthcare provider must follow its breach reporting obligations under HIPAA, which includes notification to affected patients as well as the Secretary of HHS. In certain circumstances, a healthcare provider may be required to notify the media of a HIPAA breach if more than 500 individuals are affected.

It is critical that healthcare providers respond promptly to any ransomware attacks and work with their team of trusted advisors to follow the requirements under HIPAA and the guidance issued by HHS in order to mitigate the damage caused by a ransomware attack.

Kimberly T. Boike, Esq., is a principal at the Chicago office of Chuhak & Tecson, PC where she practices healthcare law. Ryan A. Haas, Esq., is a principal and general counsel at the Chicago office of Chuhak & Tecson where he practices employment law affecting healthcare providers.