Claire Rosston

Associate
208.383.3960
Boise
ccrosston@hollandhart.com

The Rising Cost of Ransomware Attacks: Add Breach Notification Expenses Per HHS Guidance

Publication — 8/15/2016

A Cybercriminal Is holding Your ePHI for Ransom. What Just Happened?

You've just become the victim of an age-old crime with an electronic twist. Cybercriminals are infecting computers with ransomware using infected websites and emails with malicious attachments or links to infected webpages. Ransomware will encrypt all data within your computer's reach, including accessible electronic protected health information (“ePHI”). Until you pay the ransom to receive the decryption key, your data is held hostage. Unfortunately, recovery of the encrypted data without obtaining the decryption key is highly unlikely due to the cybercriminal's well-implemented, strong encryption. Plus, some victims have paid ransoms and still been denied a decryption key. Some ransomware also destroys or surreptitiously transfers your data. Recent guidance from the HHS Office of Civil Rights (“OCR”) makes it clear that a ransomware attack usually results in a breach under HIPAA that requires compliance with costly notification rules. The OCR's recent ransomware guidance is available at www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

What Should You Do?

OCR's recent guidance confirms ransomware attacks are security incidents, requiring you to initiate your security incident response and reporting procedures upon detection of the attack. Under these procedures, you should:

1. **Analyze** – Conduct an initial analysis of the scope, origin, status, and methodology of the ransomware.

2. **Isolate and Preserve** – Remove the infected computers from the network to avoid propagation on the network to file servers. Do not clean or re-image the infected computers. If other recovery approaches do not work, these computers may be your last option for recovering your data.

3. **Recover** – Restore the data lost and return to normal operations. Ideally, you have a backup drive physically stored offline. Ransomware can encrypt any data on any drive, including backup drives, and some versions of ransomware can lock cloud-based backups when systems continuously back up. The FBI does not recommend paying the ransom, but acknowledges businesses will consider all options when faced with the inability to function.

4. **Report** – Notify the affected individuals, the Secretary of HHS, and the media (for breaches affecting more than 500 people only) in

compliance with the applicable HIPAA breach notification rules. HIPAA defines a breach 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.” According to the OCR's recent guidance, a breach occurs when ePHI is encrypted by ransomware because unauthorized individuals have taken possession and control of the data and it is presumed that the ePHI has been compromised unless proven otherwise by a risk assessment. A detailed guide for responding to HIPAA breaches is available at https://www.hollandhart.com/responding-to-hipaa-breaches.

How Do You Establish A Low Risk of Compromise to Avoid the Breach Notification Requirements?

You must conduct a thorough risk assessment that is completed in good faith and results in sufficient documentation to support your reasonable conclusion given the circumstances that there is a low probability that the ePHI has been compromised by the ransomware. At a minimum, the risk assessment must consider: (a) the ePHI involved, (b) the unauthorized person to whom the disclosure was made or who used the ePHI, (c) whether the ePHI was actually acquired or viewed, and (d) mitigation of the risk to the ePHI. In the context of ransomware, this fact-intensive analysis should focus on correctly identifying the malware involved, the algorithmic steps undertaken by the malware, communications with the cybercriminal's command and control servers, and propagation to other systems. This can help determine, among other things, what types of data was searched for, whether the original data was encrypted, whether there were attempts to transfer the data, and whether hidden malicious software was implanted to provide future unauthorized access. Without offering any examples or bright lines for deciding whether there is a low risk of compromise, the OCR's recent guidance encourages you to consider additional factors concerning the high risk of unavailability of ePHI and the impact of the ransomware on the integrity of ePHI.

Is Reporting Required for Encrypted ePHI?

The HIPAA breach notification provisions do not apply to ePHI that have been encrypted consistent with the *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* (see www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html) as long as the implemented encryption in fact rendered the ePHI unreadable, unusable, and indecipherable to unauthorized persons. Full disk encryption satisfies this standard when the infected computer is turned off but does not limit access to cybercriminals who gain the same access levels granted to an authenticated user who opened the malicious attachment or performed another action that enabled the ransomware to access the files containing ePHI. Encrypting ePHI in accordance with HHS guidance is not enough. Your encryption methodologies must have actually rendered the ePHI unreadable, unusable, and indecipherable to the cybercriminals.

What Else Can You Do to Protect Yourself from Ransomware?

Visit this article for a discussion a more detailed discussion of methods for protecting yourself against ransomware. The Federal Trade Commission's recent *LabMD* decision highlights the importance of data security and makes clear that healthcare entities may incur regulatory action by either the FTC, HHS, or both for lax cybersecurity practices (see this article).