HEALTH LAW ALERT

8/15/16

HHS Issues Guidance on Ransomware Attacks

By David J. Hochman, Partner

In July 2016, the Department of Health and Human Services Office of Civil Rights issued guidance ("HHS Fact Sheet") intended to help health care entities understand and respond to ransomware attacks.[1] Ransomware is a type of malware that denies a user's access to its electronic data by encrypting the data with a "key" known only to the hacker. After the malware is deployed, the hacker demands that the user pay a ransom (usually in cryptocurrency, such as Bitcoin, to enable the hacker to preserve anonymity) to obtain the key and decrypt the data. If the ransom is paid, there is no assurance that the perpetrator of the ransomware will provide the necessary key or will not destroy or exfiltrate the user's data.

According to the HHS Fact Sheet, there have been 4,000 daily ransomware attacks since early 2016. This is a 300% increase over ransomware attacks reported in 2015. The FBI has stated that in the first three months of 2016, $209 million was paid to satisfy ransomware demands. This is most likely understated, as many successful ransomware attacks are never reported because the victims are embarrassed or have paid the ransom and were able to recover their data.

The HHS Fact Sheet makes it clear that when electronic protected health information ("ePHI") is encrypted by ransomware, a disclosure which is not permitted under the Health Insurance Portability and Accountability Act ("HIPAA") occurs, because possession or control of the ePHI is acquired by unauthorized individuals via the attack. Whether this is a breach under HIPAA, is a fact-specific determination. Unless the **c**overed entity or business associate (both of which are parties required to comply with HIPAA) can show that there is a "low probability that the PHI has been compromised," a breach of ePHI is presumed to have occurred as a result of the ransomware attack. If it cannot be determined that there is a low probability that the ePHI has been compromised, the covered entity must notify those individuals whose ePHI may have been disclosed, the Department of Health and Human Services and, for breaches involving over 500 individuals, the local media.

To determine whether a ransomware attack results in a low probability that a reportable breach has occurred, an assessment should be conducted based on the factors set forth in the HIPAA Breach Notification Rule. Such an assessment must consider, at a minimum, the following four factors:

- Nature and extent of the ePHI involved, including the types of identifiers and the likelihood of re-identification;
- Unauthorized person who used the ePHI or to whom the disclosure was made (Ransomware may not only encrypt a user's data, it may also export it from the user's computer system);
- Whether the ePHI actually was acquired or viewed; and
- Extent to which the risk to the ePHI has been mitigated.

The HHS Fact Sheet also encourages affected entities to look at additional factors to assess the risk that ePHI has been compromised by the ransomware (e.g., if there a high risk the data will be unavailable and the data's integrity has been compromised, this may indicate the data has been compromised).

[1] FACT SHEET: Ransomware and HIPAA.

It is important to note that the HIPAA breach notification requirements only apply to "unsecured" PHI. HHS' *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable*[2] provides that if ePHI is encrypted in a manner such that it is no longer deemed "unsecured", a risk assessment is not necessary to determine if there is a low probability that the ePHI has been compromised, and, therefore, a breach notification is not required. But even if the ePHI has been encrypted in compliance with HHS guidelines, it may be necessary to make a further analysis to determine that the encryption has rendered the ePHI inaccessible to unauthorized persons. The HHS Fact Sheet describes a situation in which encrypted data may still be compromised. For example, a full disk encryption solution may render computer data on a hard drive unreadable, unusable and undecipherable to unauthorized persons while the computer system is powered down; however, once the computer system is powered on and the operating system is loaded, many full disk encryption solutions will transparently decrypt and encrypt files accessed by the user. In that situation, the entity would need to make a risk assessment to determine if there was a low probability of compromise of the ePHI and provide the required notice if that assessment shows that there was more than a low probability.

The guidance from HHS reiterates how security measures required to comply with HIPAA can help covered entities and business associates prevent ransomware and other malware attacks. The required security measures include:

- Implementing a security management process which includes conducting a risk analysis to identify threats to ePHI and implementing security measures to mitigate or remediate those risks;
- Implementing procedures to guard against and detect malicious software;
- Training users on malicious software protection so they can assist in detecting malicious software and know how to report such detection; and
- Implementing access controls to limit access to ePHI to only those persons or programs requiring access.

While the HHS Fact Sheet discusses actions which an entity should take if a ransomware attack is discovered before the data is encrypted, it does not address whether there are any circumstances under which the ransom demanded should be paid. In May of this year, the Kansas Heart Hospital suffered a ransomware attack. The hospital paid a small amount to the hacker, but after this payment, the hacker would not return full access to the files and demanded an additional payment, which the hospital did not make. In a separate incident, Hollywood Presbyterian Hospital paid a ransom of $17,000, although the attackers initially demanded $3.4 million. The increasing incidence of ransomware attacks makes it imperative that covered entities and business associates review and improve their security procedures on a continuing basis.

If you have any questions on the HHS Fact Sheet or HIPAA compliance obligations, please contact one of the listed Roetzel attorneys.

Author
David J. Hochman
dhochman@ralaw.com

Additional Contacts
Ericka L. Adler
eadler@ralaw.com

[2] A copy is available at www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.

Christina M. Kuta
ckuta@ralaw.com

Media Contact
Ashley McCool
amccool@ralaw.com