# Protecting Your Practice from Ransomware

Blog | March 15, 2017 | Compliance, HIPAA, Patient Confidentiality

**By Ericka L. Adler**

Most physicians are aware of the Health Insurance Portability and Accountability Act (HI
protected health information (PHI). However, many practices are still non-compliant witl
for Economic and Clinical Health (HITECH) requirements of HIPAA, which are cumbersome and expensive for the average practice to satisfy.

How many physicians have ever heard of "ransomware" or are familiar with how to prevent a ransomware attack to their practice? Ransomware is a type of malware (malicious software), which attempts to deny access to a user's data. This can be done by encrypting the data with a key that is known only to the hacker who sent the malware. Until a ransom is paid, the key to access the data is not provided. Typically, the "ransom" is paid in a cryptocurrency such as bitcoin. However, some hackers use ransomware to also destroy or remove the data within the system.

Ransomware is a significant issue for healthcare providers. According to the Department of Health and Human Services (HHS) Fact Sheet on Ransomware, a U.S. government interagency report indicated that there were 4,000 daily ransomware attacks through 2016 (a 300 percent increase over 2015). Moreover, according to HHS, HIPAA compliance helps covered entities and business associates prevent infections of malware, including ransomware. Some of the HIPAA required measures (under the Security Rule) that assist in this protection include:

1. Implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic PHI (ePHI) and implementing security measures to mitigate or remediate those identified risks;

2. Implementing procedures to guard against and detect malicious software.

3. Training users on malicious software protections so they can assist in detecting malicious software or know how to report such detections; and

4. Implementing access controls to limit access to ePHI to only those persons or software programmers requiring access.

Practices should not only meet the above requirements (as well as the additional requirements spelled out in the HIPAA security rules), but should also maintain frequent backups of all ePHI and ensure the ability to recover such data from backups. This will help a practice be able to quickly recover from a ransomware attack. This backup ability should also be tested periodically. Since ransomware has also been known to remove or disrupt online backups, covered entities should also consider maintaining backups offline and unavailable from their networks. Although it may sound overwhelming (and expensive) to establish and maintain these types of protocols, qualified IT providers can easily help a practice meet these requirements and the cost is often less than expected.

Finally, the presence of ransomware may, but does not always mean, a breach of HIPAA may have technically occurred. A breach under the HIPAA rule is defined as the "acquisition, access, use, or disclosure" of PHI in a manner not permitted under the HIPAA Privacy Rule, which compromises security or privacy of the PHI. When ePHI is encrypted as a result of a ransomware attack, a breach has technically occurred because the ePHI was acquired by those who are not authorized to have possession or control of the information. This is clearly a "disclosure," but does not rise to the level of a breach if the covered entity or business associate can demonstrate that there is a low probability that the PHI has been compromised (based on factors set forth in the breach notification rule). The covered entity must make the appropriate analysis and comply with the applicable HIPAA requirements.

Every practice should take steps to make sure appropriate protections are in place so as to be fully compliant with HIPAA Security Rule. Although satisfying the full requirement of HIPAA to avoid ransomware may seems like a complicated and expensive undertaking, the consequences of not complying may be far greater.