Published on *The National Law Review* https://natlawreview.com

New HIPAA Guidance on Ransomware Prevention and Recovery

Article By:

Rose Willis

A U.S. government interagency report indicates that there has been a 300 percent increase in the daily ransomware attacks in 2016 as compared to 2015. Ransomware is malicious software that, when introduced into a system, gives a hacker access to the user's system, and the ability to encrypt data and hold it hostage until payment is received. The data is decrypted only when a ransom, usually in the form of cryptocurrency (such as bitcoin) is paid. If and when it is decrypted, the original data is gone leaving only the data in encrypted form.

Healthcare data is an ideal target for hackers. If you are a covered entity or business associate under HIPAA, you must take preventive action to defend against ransomware attacks. The key to such prevention is the implementation of effective security measures under the HIPAA Security Rule.

New guidance issued by the Department of Health and Human Services, entitled "Fact Sheet: Ransomware and HIPAA" (Guidance), answers various questions relating to preventing and responding to ransomware attacks.

The Guidance emphasizes the importance of implementing HIPAA Security Rule requirements, including the following key measures:

- Conducting a thorough and accurate risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified 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 detections.
- Implementing access controls to limit access to ePHI to only those persons or software programs requiring access.
- Implementing a data backup plan and ensuring the integrity of the backed up data by conducting test restorations. Maintain data backups offline if possible because some

ransomware variants have been known to remove or otherwise disrupt online backups.

The Guidance also reminds us that the presence of ransomware (or any malware) on computer systems is a “security incident” that could be considered a reportable breach under the HIPAA Rules. Security incidents must be addressed under the entity’s security incident procedures and response and reporting processes. Whether the security incident is a breach is a fact-specific inquiry. The extent that the entity has encrypted its ePHI will be a key factor in determining whether the presence of ransomware is a reportable breach.

National Law Review, Volume VI, Number 201