Codify
BY AAPC

Health Information Compliance Alert

Case Study: Ransomware Continues to Be a Thorn in Healthcare's Side

Check out new guidance and information about the WannaCry hack.

When a malicious virus corrupts your practice systems, you lose more than just your patients' ePHI. You lose the ability to practice medicine safely, running the risk of more than just the loss of privacy.

Background: Last month, a large-scale ransomware attack fanned out across much of Europe and Asia. The situation escalated quickly, and without access to medical records, patients were turned away from clinician practices, clinics, and hospitals. As the hack unfurled, federal reports indicated that the U.S. had also been impacted by the "WannaCry" ransomware infiltration, which demanded payment in bitcoin to decrypt the data.

"HHS is aware of a significant cybersecurity issue in the UK and other international locations affecting hospitals and healthcare information systems," said **Laura Wolf**, chief of the critical infrastructure protection branch, HHS Office of the Assistant Secretary for Preparedness and Response (ASPR). "We are also aware that there is evidence of this attack occurring inside the United States."

Definition: Data-for-ransom is the latest fad in the hacking world. Ransomware hackers breach servers, networks, and systems encrypting files containing documents and ePHI, then demand a ransom in exchange for the remedy needed to decrypt the files. And this type of malware (short for malicious software) causes mayhem, particularly for healthcare workers, who need precise data to safely care for patients.

"Ransomware is a virtual stick-up," explains Providence-based attorney **Steven Richard, Esq.**, with Nixon Peabody LLP. "Hackers essentially try to find the weakest links in your system to be able to take your data, hold it hostage, and make you pay a ransom to be able to obtain and use it in the future."

"Unsuspecting workers will click on a link or an email and consequently infect your system with encryption that prevents access," Richard says. "Hackers typically target the most data-dependent businesses, such as healthcare or governmental functions, where the data has the most value and the ransom can be the most threatening."

What is "WannaCrypt" Ransomware?

The malware named "WannaCry" formerly called "WannaCrypt" and shortened to "WyCry" in the media impacts Microsoft products, specifically Windows XP, and accesses data from an earlier attack on the U.S. National Security Agency (NSA), a May 2017 news release from Microsoft suggests. A patch was distributed back in March to combat the earlier hack, but many users didn't properly update their systems.

"Microsoft had released a security update to patch this vulnerability and protect our customers. While this protected newer Windows systems and computers that had enabled Windows Update to apply this latest update, many computers remained unpatched globally," said attorney **Brad Smith, Esq.**, Microsoft President and chief legal officer in a blog post. "As a result, hospitals, businesses, governments, and computers at homes were affected."

Read the Microsoft blog post on the WannaCry ransomware attack at: https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/#sm.0001840zub15lff15yx2vjmnzvtts.

Federal advice: "We are working with our partners across government and in the private sector to develop a better understanding of the threat and to provide additional information on measures to protect your systems," Wolf indicated in her statement. "We advise that you continue to exercise cybersecurity best practices particularly with respect to email."

Unfortunately, the most recent updates suggest that some covered entities are still reeling from the aftershocks of the attack. "HHS is aware of two, large, multi-state hospitals systems that are continuing to face significant challenges to operations because of the WannaCry malware," said a ASPR news release from June 2, 2017 on the ransomware issue.

The HHS Office for Civil Rights (OCR) offers guidance on identifying malware in your systems with specific advice on combating a ransomware attack. The OCR fact sheet reminds covered entities that following HIPAA, specifically the Security Rule guidelines, will help you combat possible attacks. See the fact sheet at: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf.

Remember: Preparation is key to combating an attack like WannaCry. And if you are privy to a malicious hack, the first thing the OCR will look for is how you've applied the HIPAA Security Rule requirements to the management of your systems. Assess your risks first and analyze where you are dropping the HIPAA security ball, then manage those issues and implement a comprehensive, documented plan.

Block and disable: In addition to the guidance from ASPR and OCR, the U.S. Computer Emergency Readiness Team (U.S.-CERT) updated its website with links to the various Microsoft patches as well as offering insight on how to block and disable a server message block (SMB).

Reminder: "Healthcare institutions are in a tough space," says **Larry Whiteside, Jr.**, Vice President of Healthcare and Infrastructure for Optiv, a Denver-based cybersecurity solutions firm. "They have low margins and have to figure out how to spend their money wisely. Security has for decades been their last choice of spend." But as the stakes continue to rise as more and more in the healthcare industry come under the gun of cyber criminals, the time to implement defense measures is now.

Resources: To read the U.S.-CERT alert on WannaCry, visit https://www.us-cert.gov/ncas/alerts/TA17-132A.

For a closer look at the HHS Office of the Assistant Secretary for Preparedness and Response cyber threat update, visit https://asprtracie.hhs.gov/documents/newsfiles/NEWS_06_02_2017_06_15_21.pdf.