Protecting Your Health Data Against Ransomware

By: Trish Harkness, CISSP, CHPS

Ransomware is the newest threat to emerge against electronic protected health information (ePHI). Oxford Dictionaries defines ransomware as "a type of malicious software designed to block access to a computer system until a sum of money is paid". Crypto ransomware will encrypt data and locker ransomware prevents users from being able to access the information; either way, access to important data is denied and healthcare operations are interrupted. In several recent healthcare scenarios, including Hollywood Presbyterian Medical Center, a ransom in bitcoin has been demanded. Bitcoin is "a type of digital currency that uses state-of-the-art cryptography, can be issued in any fractional denomination, and has a decentralized distribution system" which is often preferred by hackers due to its anonymity compared to centralized banking.

As the old saying goes – "an ounce of prevention is worth a pound of cure". There are many ways that a practice can protect their health data and it begins with prevention. As with most security efforts, a multi-layered approach is often the most effective.

1. Encrypt ePHI at rest – While this seems like the most obvious solution, this step alone may not sufficient as it may be difficult to determine all of the locations where ePHI resides (such as Word or Excel files stored on shared network drives) or it may not be available from your EHR vendor. Also, improperly configured encryption that stores and/or transmits the decryption key in plain text can leave data vulnerable. Data encryption is different than data masking or password protecting data; thus, data protection capabilities vary by vendor. Also, encryption of ePHI databases may slow access to data because data has to be retrieved, decrypted and then re-encrypted after use.
2. Backup your health data regularly on an off-network device – If your current backup is connected to your network, consider backing up periodically to an encrypted external hard drive that is removed from the network after the backup is complete. Then, if a hacker encrypts the data on your computer and any connected network drives, you can still restore a copy of your data. You must, of course, ensure that the encryption key is also available offline (and securely stored) so that you can decrypt your backup data if needed. The frequency of your off-network backup is dependent on restore points that have been identified by the organization and is often based on the maximum amount of data that could be lost without significantly impacting the organization.
3. Technical controls for prevention – One of the primary means of delivery for a malware attack is email. (Malware is a general term for malicious software that includes viruses, Trojan horses, ransomware, etc.) Authenticating inbound emails using sender identity technologies increase the likelihood, when properly configured, that damaging email is stopped before it reaches the recipient. Additionally, scanning email for malicious software can detect potentially damaging content. Enabling a web-filter to eliminate access to inappropriate or suspicious websites can also be beneficial. Blocking ads on websites can also reduce the risk of a user clicking an advertisement infected with malware. Limiting a user's permission to run executable files may also prevent the malware from installing.
4. Train staff to be cautious of suspicious email attachments and inappropriate websites – Include basic Internet usage safety guidelines in your staff training and repeat the training at least annually. For example, do not open email links from someone you do not know or that look suspicious even if they are from someone you know. Look at the sender's email address, not just their name, to verify that the email appears to be legitimate. If in doubt, contact the sender prior to opening the attachment. Educate staff to limit website access at work to websites required to perform job

functions. If possible, completely eliminate personal use of computing resources provided by your organization.

5. Ensure that endpoint protection systems are properly installed and configured on devices with access to ePHI – Endpoint protection includes anti-malware and may specify anti-virus and/or anti-ransomware capabilities; additionally, endpoint protection may also include a firewall and/or intrusion prevention. Ensure that endpoint protection system definitions are updated frequently and the updates are pushed to all devices on the network.
6. Keep your operating system and software applications patched – Ensure that operating systems (such as Windows or iOS) are patched routinely. Avoid the use of operating systems (such as Windows XP) that are no longer patched by the vendor. Also, make sure that software applications such as Adobe, Java, etc. are patched routinely since commonly used applications are often the target of malicious software.
7. Remove an infected system from your network immediately – As soon as malware is suspected, train your staff to remove the device from your network. This may involve turning off the wireless and/or Bluetooth capability of the device, unplugging the network cable, and/or turning off the potentially infected device until it can be examined by a security expert. In addition, if you have access to file monitoring technology, look for distinctive rapid file overwrite patterns that could indicate a malware infection. If you can catch an attack early on a computing device, the device can be quarantined and removed from the network before enterprise-wide damage can be done. Earlier versions of ransomware could be removed from computing systems so that files could be restored; however, more recent rounds of ransomware are more sophisticated and may be impossible to remove without fully reformatting the computing device and losing any stored data that was not properly backed up.
8. Ideally, do not pay the ransom – If it is possible to restore your data, focus your efforts on data restoration rather than paying the ransom. Paying the ransom trusts that the hackers/extortionists that compromised your system will help you unlock the files. In addition, paying the ransom provides more financial resources to hackers/extortionists to continue developing more advanced malware attacks. "These kinds of ransomware attacks will surely continue, unless and until cybercriminals no longer have the financial incentive for taking data hostage in the first place" (Greg Slabodkin, Managing Editor of Health Data Management). Of course, if your only option to recover your data is to pay the ransom, you may have no other feasible choice.

Resources:

- Sherman, Matt. Symantec Thought Leadership's "Ransomware Do's and Dont's: Protecting Critical Data". February 28, 2015.
- Slabodkin, Greg. Health Data Management's "HIT Think: Healthcare must offer united front against ransom demands". March 30, 2016.
- Snell, Elizabeth. Health IT Security's "Understanding Ransomware and Healthcare Data Security". March 25, 2016.
- Thompson, Cadie. Tech Insider "5 ways to protect yourself against the 'ransomware' that's taking over the internet". February 23, 2016.
- Vijayan, Jai. Dark Reading's "Here's How To Protect Against A Ransomware Attack". February 4, 2016.