afmc SM
HIPAA WATCH

MAY 2019

Securing Your Data with Encryption — Data in Motion

Second of two articles in a series about data encryption

The best way to secure electronic protected health information (e-PHI) is to convert it into a format that is not readable or usable by unauthorized people. This conversion process is known as encryption. The HIPAA security rule defines encryption as a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (type of formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text.

When working to implement encryption measures for protecting ePHI, there are two types of data to consider, data at rest and data in motion. This article will cover tips and methods for data in motion.

ITEMS TO CONSIDER:

- **Covered entities should develop and formally document policies requiring encryption of electronic PHI.** The policy should address situations where encryption is required. These situations should be identified based on risk. In addition, the policy should outline the minimum level of encryption required for electronic PHI at rest and in transit.
- **Covered entities should implement strong encryption on wireless networks if they are used to transmit electronic PHI.** Wireless networking technology continues to evolve, as does the security around these networks. Because of longstanding identified weaknesses in some encryption keys, organizations must research encryption methods which reasonably and appropriately protect electronic PHI in transit. These mechanisms should be revisited as wireless security evolves.

COMMONLY USED ENCRYPTION PROTOCOLS UTILIZED FOR DATA IN TRANSIT INCLUDE:

- **Secure/multipurpose internet mail extensions (S/MIME):** Email can be encrypted by the sender and then decrypted by the intended recipient using this protocol. Email can be read only by the sender and the intended recipient.
- **Internet protocol security (IPsec):** A suite of network layer security protocols frequently used to establish virtual private networks (VPN). They enable only the two ends of a communication in a computer network to understand the encrypted messages exchanged between them.

- **Secure shell (SSH):** A cryptographic network protocol for secure data communication. It connects via a secure channel over an insecure network, a server and a client running SSH server and SSH client programs. SSH is typically used to log into a remote machine and execute commands, but it can also be used for secure file transferring. SSH also supports secure copying of files from a local computer to a remote computer or between two remote computers.
- **Secure Sockets Layer (SSL) protocol and Transport Layer Security (TLS):** Are the primary end-to-end security protocols used to protect information passing through the internet. The common scenario for these protocols is a web browser, acting as a client for the end user, interacting with a web server. Using SSL and TLS, encrypted messages between a web browser and a web server cannot be decrypted by any unauthorized party. These protocols are often identified by a small padlock symbol in the browser address bar. Any URL which uses 'https://' instead of 'http://' is using secure HTTP. Unlike the lock symbol, the presence of 'https' does not mean that all information is being sent encrypted, rather that it might be. SSL also supports File Transfer Protocol (FTPS) which adds an additional security measure than SSH File Transfer Protocol (SFTP) by generating a warning if the certificate is not valid. The client can choose to accept the certificate or reject the connection.

The encryption protocols mentioned above utilize private key encryption, public key encryption or a combination of both.

- **Private key encryption:** Users share a copy of the same key that is used to encrypt and decrypt the message.
- **Public key encryption:** Uses two keys to encrypt/decrypt a message. The sender requests the public key from the receiver and uses it to encrypt the message. They then send the message to the receiver who then uses their private key to decrypt the message.

It is very important to use secure encryption keys. The longer the key, the harder it is for an unauthorized user to decrypt and access the information. Cryptanalysis is the term used for the process of trying to read an encrypted message. Implementing strong encryption is important, but it's only the first step in protecting your data. These additional steps should be utilized on a regular basis to ensure that your procedures are current and effective:

- **Routinely check** files from your data repositories and removable media like backup tapes and audit logs to verify the electronic PHI is encrypted (unreadable)
- **Observe** wireless transactions in real time to confirm the data is encrypted during transit
- **Verify** that your network accepts only trusted keys and certificates
- **Check** that your protocols do not support insecure or outdated versions or configurations
- **Periodically examine** user access lists to verify that cryptographic key access is restricted to the fewest number of custodians possible

End users should never send unprotected electronic PHI via:

- **Unsecure email**
- **Chat**
- **Instant messaging**
- **Unsecure text messaging**
- **Unsecure wireless networks** (such as public networks)

When dealing with encryption, whether data at rest or data in motion, it is best to consult an IT specialist. Encryption is complex, and it is important that you are working with a reputable vendor that understands the specific encryption requirements mandated by HIPAA.

FOR MORE INFORMATION:

HIPAA Security Series: 4 Security Standards
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf?language=es

HIPAA Compliance Review Analysis and Summary of Results
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/cmscompliancerev08.pdf
https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/cmscompliancerev09.pdf

AHIMA encryption basics
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048923.hcsp?dDocName=bok1_048923

For more information about this issue of **AFMC *HIPAAwatch***,
or AFMC's Security Risk Analysis (SRA) services,
contact AFMC at **SRA@afmc.org** or 501-906-7511.