afmc℠
HIPAA WATCH

MAY 2019

Securing Your Data with Encryption — Data at Rest

First 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 useable 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. (45 CFR 164.304). The confidential process or key used to access encrypted e-PHI must be kept secure.

When working to implement encryption measures for protecting ePHI, there are two types of data to consider. Data at rest and data in motion.

Data at rest is data that is not actively moving, but is being stored on a hard drive, laptop, flash drive or achieved/stored in some other way. The data is inactive but has the potential to fall into the wrong hands. Resting data is less vulnerable to attack but needs encryptions measures.

Data in motion or data in transit is data actively moving from one location to another such as across the internet or through a network. The data in motion is more vulnerable to exposure and interception and is less secure while in motion.

Unprotected data, whether in rest or in motion leaves covered entities (CEs) vulnerable to attack. Each has its own risk profile and methods of protection. One of the most effective data protection methods for both is encryption.

This article will cover tips and methods for data at rest and article two in the series will cover data in motion.

WHY ENCRYPT LAPTOPS AND OTHER MOBILE DEVICES?

- **Compliance:** While the use of encryption is not mandatory under the Security Rule, it is an addressable specification, which means that after the SRA is performed, the covered entity must complete one of the following actions, depending on the results of the SRA:
    - If encryption is found to be a reasonable and appropriate safeguard in the entity’s management of the confidentiality, integrity and availability of e-PHI, then it must be implemented.
    - If encryption is not reasonable or appropriate, the entity must document the reasons why and implement an alternative that is reasonable and appropriate.
    - If the standard can be otherwise met, then the entity can choose not to use encryption or an alternative and must document the rationale for the decision.

- **Avoid data breach reporting and fines:** If a covered entity or business associate discovers e-PHI is compromised, an investigation should be conducted. AFMC offers a breach assessment tool as part of the security risk analysis process for PHI and HIPAA compliance that can be used to complete the investigation. If during the investigation it is found that the compromised PHI was encrypted, rendering it secure, then the compromise is not considered a reportable breach. The Department of Health and Human Services (HHS) continues to assess fines for breaches involving unencrypted laptops and mobile devices. This could have been avoided with the use of proper encryption.

WAYS TO ENCRYPT STORED DATA

- **Full disk encryption:** The process of encrypting all the data on the hard drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication, such as entering the correct user name and password after the computer is turned on. Full disk encryption is often considered the most secure, since access to data and the operating system is limited if the machine is lost or stolen.
- **Virtual disk encryption:** The process of encrypting a file called a container, which can hold many files and folders, and permitting access to the data within the container only after proper authentication is provided, at which point the container is typically mounted as a virtual disk.
- **Volume encryption:** The process of encrypting an entire logical volume and permitting access to the data on the volume only after proper authentication is provided. A logical volume can contain one or more containers. Volume and virtual disk encryption can be used to protect data from specific users when a device is shared, or in the event the device is lost or stolen. It can also be used to encrypt a container or volume of data before storing on a USB or other portable device.
- **File/folder encryption:** The process of encrypting individual files or folders on a storage medium (e.g., hard drive, thumb drive) and permitting access to the encrypted data only after proper authentication is provided. If using a single sign-on, this usually means the files are only protected until the user logs on. This type of encryption can't protect the confidentiality of file names or other metadata of the file.
- **Combination:** A combination of the above types of encryption may be used to protect against many classes of threats.

KEY CONSIDERATIONS AND BEST PRACTICES FOR ENCRYPTION

- **Consult with your IT support staff or an outside IT professional.** Incorrectly installing, configuring or using encryption can render your data permanently inaccessible.
- **Do your homework.** Read about the encryption product. Understand what it will do for you, and how it should be configured.
- **Encryption is dependent on the use of strong passwords.**
- **Ensure your encryption solution comes from a reputable company.** Avoid using an encryption product that uses proprietary algorithms. There are excellent solutions based on publicly known algorithms such as Advanced Encryption Standard (AES) or Blowfish.
- **Encrypted data can become permanently lost if you forget the password.**
- **Encryption is a must for laptops, smartphones, tablets and other mobile devices.** These devices are easily lost or stolen.
- **Encryption software must be maintained with appropriate updates to ensure reliability.**
- **Regularly back up confidential data.** This will ensure that if you lose your device or the encryption key (password) protecting your data, you can recover your data.

Regardless of which type encryption you are using or how you use it, encryption is only effective if you have strong passwords and maintain the overall security of your computer. Encryption does not protect against viruses, worms, Trojan horses or social engineering attacks. If your computer is compromised, so is your data.

RESOURCES:

Department of Health and Human Services
hhs.gov/ocr/privacy/hipaa/faq/securityrule/2001.html
hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/

Guidance to Render Unsecured Protected Health Information Unusable, Unreadable or Indecipherable to Unauthorized Individuals
https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html

National Institute of Standards and Technology
csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

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.