American Professional Agency

RISK MANAGEMENT

IN THIS ARTICLE

PREPARED BY

Allison M. Funicelli, MPA, CCLA, ARM
Senior Risk Management Consultant
Risk Management Group,
AWAC Services Company,
a member company of Allied World

CONSIDER THIS ...

Encryption – What Is It, Why Do We Need It and Where Do We Get It?

In a world of continuous cyber breaches and the potential for mishandling of sensitive data, particularly Protected Health Information (PHI) and Personally Identifiable Information (PII), keeping sensitive data secure is imperative. A loss or misuse of sensitive data can have significant social and financial consequences for both a patient and the psychiatrist.

One key way to secure sensitive data is through encryption. Encryption converts information from a readable format to an encoded format to prevent unauthorized users from accessing it. In order to access encrypted data, the user needs the decryption key (typically a password or phrase) to decode the message. Passwords alone do not ensure data security. Confidential and sensitive data housed on computer servers, laptops and mobile devices should be encrypted with difficult to decipher decryption keys. A decryption key should be difficult to hack. Decryption keys, such as password 1234, are easy for computer hackers to decipher and should never be used.

How Does Encryption Work?

Encrypting data undergoes five key steps when using encryption software:

- Plaintext – the original data created
- Encryption algorithm – computer code that converts the plaintext to ciphertext
- Ciphertext – the scrambled (or encrypted) version of the data
- Decryption algorithm – computer code to convert the ciphertext back to plaintext, once unlocked
- Decryption Key – the password used to unlock the encrypted data

There are multiple forms of encryption software that may be used, depending on the type of device (for example, hardware versus cloud servers). Extra care should be taken with portable devices that can be easily lost or stolen including laptops, tablets, mobile phones, flash drives and portable hard drives. Portable devices housing sensitive data should use encryption software.

Am I Required to Encrypt PII/PHI Under HIPAA?

The short answer is no. The HIPAA Security Rule (Security Rule) requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of Electronic Protected Health Information (ePHI). Under the Security Rule, Covered Entities (CE) and Business Associates must develop and implement policies and procedures to protect ePHI they create, receive, maintain, or transmit.[1]

The Security Rule, however, does not require encryption of PII/PHI as receiving records in an encrypted format may place an undue burden on some patients. Thus, the Security Rule allows CE's to have some flexibility with compliance of the security standards. Therefore, when a patient requests their PII/PHI in an unencrypted format, the Security Rule permits the psychiatrist to send/provide PII/PHI to the patient in an unencrypted form.

However, this does not mean that a CE can ignore encryption. Specifically, the HIPAA Security Rule states, "the encryption implementation specification is addressable rather than required," and allows CEs to determine whether the addressable implementation specification is reasonable and appropriate for that CE. If the CE decides that the addressable implementation specification is not reasonable and appropriate, it must document that determination and implement an equivalent alternative measure, presuming that the alternative is reasonable and appropriate.[2]

How Do I Encrypt My Data?

- Purchase self-encrypting hard drives.
- Consult with IT professionals when purchasing, installing and maintaining encryption software.
- Consult with risk management professionals specializing in cyber liability to assess and test the security of your organization's encryption and data storage methods.
- Use multiple methods in securing your data in addition to encryption (i.e., lock devices, limit personnel access to sensitive data, train personnel in the handling of sensitive data, maintenance of data back-up in the event of loss of data).

Encryption Caveat

Unlike passwords that can be reset, decryption keys cannot be reset or retrieved. Therefore, due care needs to be taken when selecting a decryption key. If a decryption is saved in written format, care needs to be taken to keep the encrypted device or data separate from the decryption key to ensure the encrypted data remains secure from those who should not have access.

RISK MANAGEMENT TIPS:

- Create a written policy for securing sensitive data on computers and mobile devices.
- Encrypt all sensitive data, whenever possible.
- Consult IT and Cyber Risk Management Professionals in developing a comprehensive plan for securing and encrypting data.
- Train personnel on the proper use and protection of sensitive data.
- Be familiar with and comply with state and federal regulations related to securing sensitive data.
- If a patient requests their PII or PHI in an unencrypted format, explain to them the risks and potential consequences of providing sensitive data that is not secure. Document the details of the conversation with the patient in their medical record.

[1] United States Department of Health and Human Services, "HIPAA Basics for Providers: Privacy, Security and Breach Notification Rules," (May 2015).

[2] Health IT Security, "Breaking Down HIPAA: Health Data Encryption Requirements." (https://healthitsecurity.com/news/breaking-down-hipaa-health-data-encryption-requirements)

For other timely risk management topics, policyholders can access In Session, our risk management newsletter, at apamalpractice.com.

If you have any questions please contact the American Professional Agency, Inc. at 877-740-1777.

apamalpractice.com

awac.com/risk_control

IN THIS ARTICLE

American Professional Agency

RISK MANAGEMENT