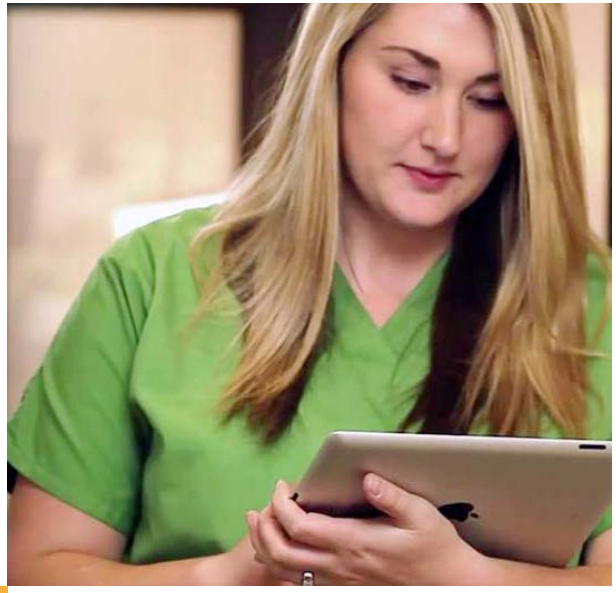
securityMETRICS®

White Paper

MEDICAL DATA ENCRYPTION 101

Safely Encrypt Your Protected Health Information



MEDICAL DATA ENCRYPTION 101

SAFELY ENCRYPT YOUR PROTECTED HEALTH INFORMATION

INTRODUCTION

If an attacker is able to break into a work device, encryption renders files useless by masking them into an unusable string of indecipherable characters. From a security standpoint, encryption is essential to keep your patients' protected health information (PHI) safe.

Unencrypted data has been the cause of fines from the HHS in the event of a breach, as in the cases of Blue Cross Blue Shield of Tennessee, Massachusetts Eye and Ear, and Hospice of North Idaho. These breaches resulted in thousands of dollars in fines and the loss of patient trust.

With this danger in mind, HIPAA requires healthcare entities to "implement a method to encrypt and decrypt electronic protected health information" in requirement §164.312(a)(2)(iv). All electronic PHI that is created, stored or transmitted in systems and work devices must be encrypted (e.g., mobile phone, laptop, desktop, flash drive, hard drive, etc.).

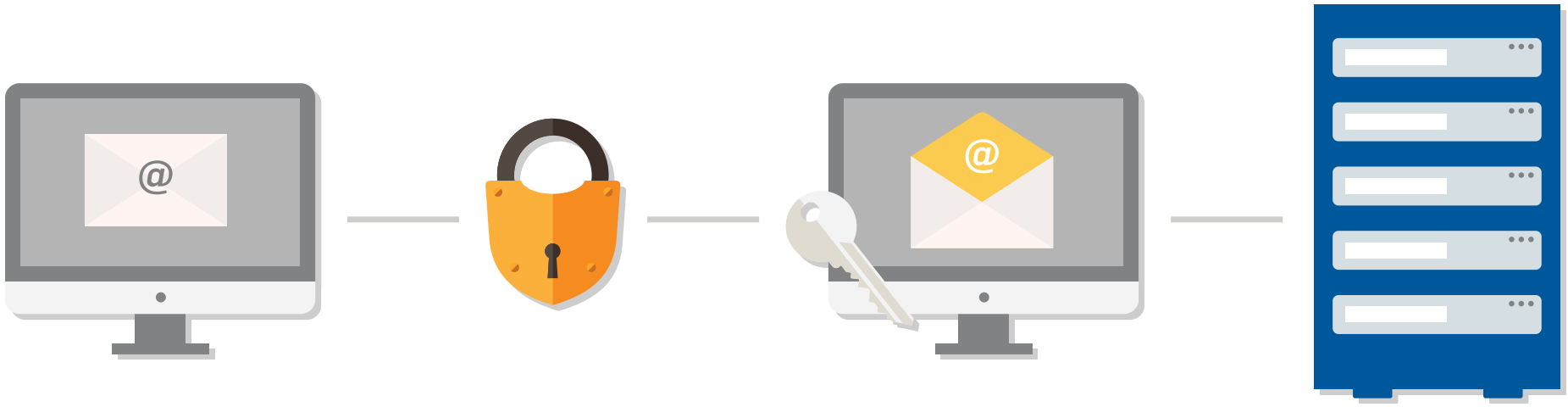
ONLY 63% OF HEALTHCARE ORGANIZATIONS ENCRYPT PHI ON THEIR WORK DEVICES.*

*SecurityMetrics HIPAA Security Rule Report

WHERE IS YOUR DATA?

In order to properly encrypt PHI, you have to understand how medical data flows within your organization, especially where PHI is stored and transmitted. To make sure all necessary data is encrypted, begin with a daigram that documents how your PHI travels throughout your organization.

YOU NEED TO DOCUMENT WHERE PHI ENTERS YOUR ENVIRONMENT, WHAT HAPPENS ONCE PHI ENTERS, AND HOW PHI EXITS.



PHI ENTRY

Identify everywhere PHI starts or enters your entity. By doing so, you know exactly where to start with your encryption practices.

Consider the following questions about where your electronic PHI enters your environment:

- Email: How many computers do you have, and who can log on to each computer? What email services are in use?
- Texts: How many mobile devices do you own, and who uses them?
- EHR entries: How many staff members do you have entering in data? Who are they? From where do they enter the data?
- New patient data: How much are patients required to fill out, and where? Front desk? In the examination room?
- Business associate communications: How do business associates communicate with you?
- Databases: How do you communicate with patients? What records and data do you enter into your database?

PHI TRANSMISSION

When PHI leaves your organization, it is your job to ensure it is transmitted or destroyed in the most secure way possible. Specifically, you and your business associate are responsible for how your business associate handles your PHI.

Here are some things to consider when PHI leaves your environment:

- Business associates: Are you sending through encrypted transmission? Are they? Is data sent to them kept at a minimum?
- Email: What procedures are in place for how patients receive data?
- Flash drives: What policies are in place?
- Trash bins on computers: How often are these cleared out?

PHI STORAGE

You need to know exactly what happens to PHI after it enters your environment. Is it automatically stored in your EHR/EMR system? Is it copied and transferred directly to a specific department (e.g., accounting, marketing)?

Additionally, you must record all hardware, software, devices, systems, and data storage locations that can access PHI. PHI is commonly stored in the following places:

- EHR/EMR systems
- Mobile devices
- Email
- Servers
- Workstations
- Wireless (networked) medical devices
- Laptops
- Computers
- Calendar software
- Operating systems
- Applications
- Encryption software

After knowing these processes, you should find gaps in your security and environment, and then properly encrypt all PHI.

AN AUDITOR'S PERSPECTIVE

ENCRYPTION–THE REQUIRED ADDRESSABLE

Even though the HIPAA regulations indicate that encryption is an addressable item, the HHS has made it very clear it's viewed as required.

Let me tell you what doesn't count as encryption. I have run into several healthcare professionals who showed me their spreadsheets of PHI saying, "See, I encrypt it when I make the cell smaller and the numbers change to '###'." Just to be clear, this is not encryption.

Three common data handling processes that are often confused: masking, hashing, and encrypting. Let me break them down for you:

- Masking is hiding part of the data from view. It is still there in clear text, you just can't see all of it on the screen. You use this to hide parts of the patient information not needed by a specific workforce member.
- Hashing is running the data through a mathematic algorithm to change it into something indecipherable. You cannot undo a hashed value to get back to the original data. Generally, healthcare doesn't hash PHI.
- Encrypting is similar to hashing because data is run through a mathematic algorithm; however, you use an encryption key that has a paired decrypting key. This way the data is safely stored and the only way to see the data is by using the decryption key to unlock it. The strongest, most common encryption algorithm is AES-256. Whenever implementing encryption, always use the strongest algorithm your system can handle. Remember that many older algorithms are not acceptable (e.g., rc4, DES). Anywhere PHI is stored you should have encryption enabled so the data requires a decryption key to view it. Most computer systems can automatically handle encryption if they are properly configured.

The National Institute of Standards and Technology (NIST) identifies and judges encryption processes used for sent information, meaning healthcare organizations must comply with NIST Special Publications 800-52, 800-77, 800-113, or others which are Federal information Processing Standards (FIPS) 140-2 validated.

Due to the complexity of encryption rules, healthcare organizations often use third parties to ensure encryption of PHI, partly because organizations are required to keep the tools for decryption on another device or location.

–Brand Barney
Security Analyst | HCISPP | CISSP | QSA

ENCRYPTING MOBILE DEVICES

Most mobile encryption services are not as secure and reliable as other devices because most mobile devices themselves aren't equipped with the most secure encryption.

Mobile technology is only as secure as a device's passcode. For example, Apple's Data Protection API only encrypts the built-in mail application on iPhones and iPads, and only after you enable a passcode. Encryption does not apply to calendars, contacts, texts, or anything synchronized with iCloud. Some third party applications that use Apple's Data Protection API are also encrypted, but this is rare.

Although encryption on mobile devices would not be adequate enough to meet HIPAA best practice recommendations, there are still other options for further securing a mobile device. Security best practice is to develop and implement appropriate mobile security policies such as:

- Mobile password length requirements
- Procedure to enable available mobile encryption on all devices
- PHI storage and access procedures
- Stolen/lost device procedures
- Bring your own device (BYOD) procedures
- Noncompliance accountability

MOBILE DEVICES REQUIRE THE SAME RESTRICTIONS AND ENCRYPTION PROCESSES AS OTHER WORK DEVICES LIKE DESKTOP OR LAPTOP COMPUTERS.

ENCRYPTING EMAIL MESSAGES

According to the HHS Breach Portal, over 100 organizations since 2009 have had PHI stolen because of inadequate email encryption. Healthcare organizations must "implement a mechanism to encrypt electronic protected health information whenever deemed appropriate" in requirement §164.312(e)(2)(ii), such as when sending unencrypted PHI in unprotected email services (e.g., Gmail, Outlook, AOL, etc.).

Organizations can send PHI via email, if it is secure and encrypted. According to the HHS, "the Security rule does not expressly prohibit the use of email for sending ePHI. However, the standards for access control, integrity and transmission security require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to ePHI."

Due to the nature of email and the struggles to properly secure it through encryption, consider avoiding the transmission of PHI via email whenever possible.

The use of patient portals is preferred for sending information to patients, and secure file transfer options are preferred for covered entity to covered entity or covered entity to business associate communications.

If you are determined to use an Internet-based email service (e.g., Gmail, Hotmail, AOL), ensure the service signs a Business Associate Agreement (BAA) with you. Understand that a BAA doesn't reduce liability. The Omnibus Rule states the covered entity is still ultimately responsible for protecting that patient data and ensuring the business associate does their part.

CONCLUSION

Encryption is vital to protect your patient's data. You need to make sure that you adequately map out where PHI enters your environment, what happens once PHI enters (and where it is stored), and exits your environment or organization. Although HIPAA regulations don't specify the necessary encryption, industry best practice would be to use AES-128, Triple DES, AES-256, or better.