HIPAA Data Security Best Practices

GO ANYWHERE®
Managed File Transfer

INTRODUCTION

A growing interest among cyberattackers in targeting sensitive health data has resulted in an increased number of health data breaches. According to Verizon's 2018 Data Breach Investigations Report (DBIR), the healthcare industry experienced 750 cyber incidents in 2017. Around 530 involved data disclosure. Medical data was the target of two-thirds of data breaches in the healthcare industry while protected health information (PHI) made up 37 percent of breaches, the report found.

The Office for Civil Rights (OCR) has often taken action against healthcare organizations with security vulnerabilities that led to data breaches. In fact, the impermissible use and disclosure of PHI has been the number one compliance issue investigated by OCR since the HIPAA Privacy Rule took effect in 2003.

The Office for Civil Rights has often taken action against healthcare organizations with security vulnerabilities that led to data breaches. In fact, the impermissible use and disclosure of PHI has been the number one compliance issue investigated by OCR since the HIPAA Privacy Rule took effect in 2003.

And OCR has not been shy about levying fines on HIPAA violators. The agency hit the University of Texas MD Anderson Cancer Center with a whopping $4.3-million HIPAA fine in 2018 for failing to encrypt its inventory of devices that handled and held electronic PHI (ePHI) of more than 33,500 individuals. New Jersey-based Virtua Medical Group recently paid close to half a million dollars for failing to protect the data of more than 1,650 individuals, while St. Elizabeth's Medical Center in Massachusetts entered into a $218,400 settlement when certain workforce members used an unsecured application to store PHI of around 500 individuals.

HIPAA violations are not the only threats to healthcare organizations. Ransomware continues to be a major concern for provider groups. A survey conducted by HIMSS Analytics earlier in 2018 found that three-quarters of providers experienced a healthcare ransomware or malware attack the previous year. In 2017, it was the WannaCry ransomware that infected medical devices and devastated healthcare organizations. WannaCry not only threatened PHI data but also patient safety.

OCR has also warned about SamSam ransomware targeting healthcare organizations. SamSam's victims included Indiana-based Hancock Health Hospital and Adams Memorial Hospital, cloud-based EHR provider Allscripts, and possibly Case Regional Medical Center.

TECHNICAL REQUIREMENTS UNDER HIPAA

The HIPAA Security Rule requires healthcare organizations to implement technical safeguards that can help protect against data breaches and ransomware attacks. There are five categories of technical safeguards: access control, audit controls, integrity, person or entity authentication, and transmission security.

Access controls provide users with rights and privileges to access and perform functions using information systems, applications, programs, or files. HIPAA requires covered entities to implement unique user identification and emergency access procedures. Where reasonable and appropriate, covered entities should also implement automatic logoff and data encryption.

The healthcare industry experienced 750 cyber incidents in 2017. Around 530 involved data disclosure. Medical data was the target of two-thirds of data breaches in the healthcare industry, while personal health information made up 37 percent of breaches.

Source: Verizon 2018 DBIR

The **audit controls** standard requires covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems containing or using ePHI. A covered entity must consider organizational factors, such as technical infrastructure and hardware and software security capabilities, to determine audit controls for information systems that contain or use ePHI.

The HIPAA **integrity** standard directs covered entities to deploy policies and procedures to protect ePHI from improper alteration and/or destruction. Where reasonable and appropriate, covered entities should put in place mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

The **person or entity authentication** standard requires a covered entity to implement procedures to verify the identity of the person or entity seeking access to ePHI. There are several ways to verify identity: require information known only to the individual such as a password or PIN, require an item that an individual possesses such as a token or key, or require an identifier unique to the individual such as a fingerprint.

The **transmission security** standard mandates that a covered entity implement technical security measures to guard against unauthorized access to ePHI being transmitted over a network. Where feasible and appropriate, covered entities should implement integrity controls to prevent unauthorized modification of ePHI in transit and data encryption during transmission.

CHOOSING APPROPRIATE MEASURES, TECHNOLOGIES

HIPAA has been updated several times since 1996, and the law continues to pose technical challenges to covered entities and their business associates with each change. While the revisions are intended to provide clarity around rapidly changing technologies, organizations are still debating the nuances of how to develop and deploy secure data management frameworks that best meet their individual needs.

"There's not any one recommended platform. There's not only one recommended security measure," says Laura Hammargren, Partner at Mayer Brown, leader of the firm's healthcare practice.

And that lack of specificity leaves the door open for interpretation by healthcare providers and their business partners as they evaluate potential technology solutions for implementation.

"You have to do what's right for your business," Hammargren continues, "which in a way makes some sense because there are so many different types, sizes, and distributions of covered entities, and types and sizes of distribution. It's hard to think of a one-size-fits-all solution or more exact standards."

> *"You have to do what's right for your business, which in a way makes some sense because there are so many different types, sizes, and distributions of covered entities, and types and sizes of distribution. It's hard to think of a one-size-fits-all solution or more exact standards."*
>
> **Laura Hammargren**
> **Partner**
> **Mayer Brown**

According to partners at law firm McDermott Will and Emery, the process of choosing the right standards and technologies will be an "organic one."

"Every covered entity and business associate should evaluate their obligations under the security rule while keeping the flexible nature of the rule in mind when determining how to implement safeguards," explains Edward Zacharias, who counsels HIPAA compliance, OCR investigation and enforcement actions, and privacy and cybersecurity risk management out of McDermott's Boston office. "There is room for a covered entity or business associate to make a determination that a particular addressable implementation specification is not appropriate for either some or all of its environment."

Documentation is key to supporting business decisions around health data security and privacy under HIPAA, especially in light of the federal government's increased push for care coordination and information sharing. As Zacharias notes, "Any decision not to adopt an addressable implementation specification should be documented in writing, with supporting evidence regarding why it was not reasonable to adopt that standard, along with a description of any compensating controls that were implemented to safeguard the information."

"You obviously want to know the nature of the interaction, whom you're dealing with and where you're disclosing information," Zacharias explains. "Where you're disclosing information, you want to have a reasonable level of comfort that the other party involved in the transaction is actually complying with its obligations under the security rule."

Zacharias has observed a marked change in the industry's discussions about health data transmission security solutions for managing data exchange.

"The conversations around the deployment of those technologies and safeguards are very similar to those we had seven to eight years ago around encryption. It is becoming less of a nuanced and unknown technology and becoming more widely available, more widely used," he adds.

Other emerging technologies allowing for real-time collaboration (e.g., Box, Dropbox, Google Drive) also present new challenges to maintaining HIPAA compliance.

"As people become more used to collaborative workspace environments (moving away from working on a secure document on your own system and then transmitting it by encrypted email or other secure means, to instead working in parallel with others on a live document on a shared system), that's going to be an ongoing challenge for maintaining a HIPAA-compliant, appropriately safeguarded operations," says fellow McDermott Will and Emery partner David Gacioch.

> *"As people become more used to collaborative workspace environments...that's going to be an ongoing challenge for maintaining a HIPAA-compliant, appropriately safeguarded operations."*
>
> **David Gacioch**
> **Partner**
> **McDermott Will and Emery**

According to Hammargren, the market is "wide open" for health data security companies to meet the needs of providers and opportunities for HIPAA-covered entities to shore up certain vulnerabilities and move on to addressing others.

Resources, however, will need to be wisely spent, because—as Hammargren admits—some providers will be hard pressed to come up with sufficient resources for costlier products. And regulators understand that,

which contributes to the lack of prescriptions in HIPAA itself.

That said, covered entities and business associates will be on the hunt for the best and most affordable solutions that ensure the exchange of PHI between trusted users and also deliver a high-quality experience for patients and consumers, from multifactor authentication to managed file transfer technologies.

BEST PRACTICES FOR SECURING PHI

With "reasonableness" as a guiding principle, HIPAA-covered entities can meet the requirements under HIPAA for access controls, audit controls, data integrity, person or entity authentication, and transmission based on the organizational and financial capabilities of their organizations.

In a recent presentation, Sentara Healthcare's Vice President and CISO Daniel Bowden identified the set of best practices the health system and plan uses to maintain high levels of health data security and privacy.

Take a proactive approach to health data security: Keeping tabs on the latest developments and industry trends will ensure that systems are online and data is available to providers and patients. Joining an organization such as the National Healthcare and Public Health Information Sharing and Analysis Center (NH-ISAC) gives covered identifies insight into new and emerging threats.

Assess current threats to the security of PHI: Internal and external threats deserve equal attention. Phishing and malware grab headlines, but malicious and non-malicious insider threats can easily expose health data when a lost or stolen device lacks encryption or users have unnecessary levels of access to patient data.

Implement methods for managing access control: The 2017 Verizon Data Breach Investigation Report showed that privilege misuse or errors are a factor in the vast majority of healthcare breaches. Privileged access management helps restrict PHI use to appropriate personnel.

Enable audit controls to gain visibility into PHI use: Monitoring access to electronic patient data allows providers to record and respond to activity within systems housing sensitive information, most notably the electronic health record.

Safeguard against unauthorized changes to sensitive patient data: Encryption and data loss prevention technology protect the integrity of PHI, especially in motion. A thorough examination of business practices will enable provider organizations to respond to and recover quickly from attempts to alter data.

Verify appropriate access to PHI for individuals and organizations: Covered entities must determine who has access to PHI and employ strong authentication and access auditing methods to ensure that data access is in line with a user's role in the organization, both present and future. Human resources has an important role to play in notifying IT of changes in employment status.

The financial implications of a health data breach are significant. Provider organizations failing to implement appropriate technical safeguards risk imperiling their current and future business.

Published by

Xtelligent Media

About HelpSystems

helpsystems

HelpSystems aligns IT and business goals to help organizations build a competitive edge. More than 13,000 organizations around the world rely on HelpSystems to solve their most pressing challenges and keep business running smoothly every day.

GoAnywhere MFT is a HelpSystems file transfer solution that uses OpenPGP or AES encryption and industry-standard protocols to comply with HIPAA and HITECH regulations. The software exchanges files via batch, collaboration, and ad-hoc methods, uses workflows to execute tasks before and/or after transfers, and offers healthcare teams multiple options for secure data exchange. Try a 30-day trial at www.goanywhere.com/trial.