Encryption in Healthcare

The Right Prescription for Maintaining Compliance with Patient Security Regulations

In the healthcare industry, expensive equipment is usually a point of pride, but one leading provider never intended to pay $1.5 million each for two laptops. Only after the laptops were stolen did it come to light that they contained over 1 million unencrypted patient records — a clear HIPAA violation. The provider ended up settling a class action suit for $3 million, but plenty of other healthcare providers have felt the sting of failing to comply with HIPAA, as well. The next major data breach isn't a matter of if, only when.

HIPAA fines and settlements are expensive, but they're just the tip of an even more costly iceberg. After HIPAA costs comes all of the other financial damage. An affected healthcare provider must foot the bill for identity theft protection/credit monitoring for individual victims. Nearly inevitable civil lawsuits will likely result in costly settlements and judgments. Depending on the size of the breach, the HIPAA settlement could be the least of a healthcare provider's worries.

Real Risk

Today, encryption is a staple of the professional world. Virtually every industry that deals with personal and/or sensitive data relies on encryption to protect that data. Service providers that don't encrypt sensitive data put themselves at risk of stiff government penalties, fines, lawsuits, and more.

Healthcare providers, insurance carriers, and others that keep and manage patient information are arguably the most targeted for malicious data breaches because patient data contains everything that thieves require to pilfer a person's identity. Stolen data can then be used to file fraudulent medical claims, open lines of credit, or preemptively claim a tax refund. With compromised healthcare data in hand, cybercriminals have essentially free rein to make profit, inflict damage, and ruin lives.

According to Ponemon's "Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data" (2015), "attacks on healthcare organizations are up 125 percent compared to five years ago." Ponemon adds that the average cost of a healthcare organization data breach now stands at $2.1 million. The first step to avoiding these expensive, potentially crippling fines and other expenses associated with a breach is to pursue regulatory compliance. HIPAA tops the list of must-observe mandates, but other regulations may come into play, as well.

Regulatory compliance entails much more than simply password-protecting an office's workstations. This article will cover how encryption applies once at-rest data leaves the firewall's protection. Indeed, "in the wild" data at rest is the top source of security breaches. According to Ponemon's 2015 study, 96% of respondents reported a security incident involving a lost or stolen device. We'll cover what a healthcare provider or associated business should and must do to move data safely on portable devices and how all of this ties into staying on the right side of HIPAA.

Chasing Compliance: How Regulations and Encryption Fit Together

Encryption is terrific…in theory. Data stays protected, and confidential information remains locked away from the wrong eyes. In reality, though, compliance costs money, whether from purchasing hardware and software, hiring a consultant, both, or possibly more. When pursuing protection, is it possible to go overboard and encrypt more than necessary?

In some instances, a particular regulation will mandate encryption in clear, unmistakable terms; failure to comply with these terms implies violation of the law. Other times, regulations may be vague about requiring encryption, leaving a gray area for businesses to decipher. For example, a regulation may dictate that sensitive and/or personal data be protected without explicitly stipulating it be protected via encryption. Obviously, these situations are less than ideal.

When the law isn't straightforward, security experts can provide clarity if and when a consensus gives way to commonly accepted best practices. The term isn't exclusive to regulations and encryption, but it can nonetheless help guide healthcare providers that encounter nebulous compliance verbiage. Following industry best practices will keep a business protected in times when the letter of the law proves hard to decipher. Sometimes, even the government will come to providers' aid with published best practices guidance, although the availability of such documents within a given niche or application can vary widely.

The Human Factor

Healthcare providers can reasonably protect themselves against known threats. For instance, they can set up firewalls to thwart incoming attacks and use virtual private networks (VPNs) and secure communication protocols, such as HTTPS, to keep data secure while in transit. In many, many cases, an entity's weakest line of defense is its own employees.

In fact, the 2015 Ponemon study indicates that respondents worry more about employee negligence (51%) than any other security threat. That's ahead of cyber attackers (35%), system failures (19%), and identity thieves (a mere 5%). Note that negligent employees aren't the same as disgruntled types, which the report classifies as "malicious insiders"; only 19% of respondents listed these employees as a chief concern.

No, the biggest threat is well-meaning but inattentive employees. They're the reason laptops containing treasure troves of data disappear. Since accidents and theft do happen with all too frequent predictability (Ponemon's 2010 paper "The Billion Dollar Lost Laptop Problem" pegs the number at 7.12% across all surveyed organizations), responsible enterprises would be playing Russian roulette by not taking appropriate precautions. Equipping portable devices with self-encrypting drives is one obvious step, but health-

Encryption and Security in Brief

Before learning how to protect data, it's useful to know a little more about the data itself — specifically where it resides. For our purposes, data exists in the following three "states": at rest, in transit, and in use. Data at rest refers to data located in persistent storage, such as a hard drive. This could be as simple as a saved document or image. Data in transit is any data sent or received across a network. Downloading a file from the Internet or transferring a file between two computers on a local area network are both cases of data in transit. Data in use is a little trickier, but it essentially means any data that a computer's CPU is actively processing or data temporarily stored within a system's RAM.

Encryption is a deep, complicated subject that many experts devote their lives to mastering, but having a rudimentary grasp of the key terms and concepts will help healthcare organizations better understand what it takes to be compliant. Ideally, sensitive data should be secure enough that unauthorized parties can't even access or obtain it. Even if data falls into their hands, though, they definitely shouldn't be able to read it. That's where encryption comes in.

Encryption transforms data to make it unreadable without authorized access. In this case, authorized access comes in the form of a decryption key, which is fairly self-explanatory. When the right people have the key, they can read your encrypted data; the wrong people who don't have the key cannot.

Many encryption methods exist, as do different instances when encryption is necessary. Encrypting data stored on a hard drive is one example, while accessing a business's network remotely over a virtual private network is another. Unfortunately, when it comes to compliance, there's no universal standard for encrypting data. The regulations that govern how each industry handles data may not dictate the same encryption requirements.

People with a passing familiarity with encryption may have heard of 128-bit, 192-bit, or 256-bit encryption. This refers to the "size" of the key, in bits, necessary to decrypt data. A 128-bit key corresponds to a total of 2128 possible keys; a 256-bit key represents 2256 possibilities. Generally, a larger key requires more time to crack via brute force methods (where an attacker uses a computer, or multiple computers, to "guess" the key). Security experts agree that it would take modern computers billions of years to brute-force a 128-bit key. Radical advancements in computing technology (quantum computing, for example) would be necessary to break 256-bit encryption.

Of all the encryption methods, AES (Advanced Encryption Standard) receives the lion's share of attention, and for good reason. The NSA uses AES to encrypt data, which ought to be proof enough of its security. AES can use 128-bit, 192-bit, or 256-bit keys and thus far has been extremely resistant to attempts at exploiting potential weaknesses. Several cryptographers have tried to break AES, but none have succeeded.

If there's a downside to AES, it would be in the computational cost of its operation. For many years, most digital encryption on computers was performed "in software," where the systems CPU performed all of the necessary encrypt/decrypt operations. This work proved exceptionally cumbersome for general purpose processors and could bring a lower-end system to its knees. Only relatively recently have Intel's AES New Instructions (AES-NI) and other innovations integrated specific encryption acceleration silicon into CPUs (thus running "in hardware") and made the burden of encryption computation negligible. This also applies to the encryption of external drives, including flash drives. Somewhere, a component crunch those encryption processes, and if there's no dedicated acceleration behind the work, other applications running on the system may suffer.

In addition to protecting data via encryption, it's important to authenticate both data and communications (i.e., transmitted files and messages) to ensure that the data received matches the data sent. Verifying data arrived from true and trusted sources is another key aspect of maintaining security, which is why security professionals recommend cryptographic hashing. A hash is a number produced from a string of text that acts like a digital fingerprint. When someone sends a message, for example, they can generate a hash and include it with the message. The recipient of the message can then create a hash of the received message and compare it with the original hash. If the two match, the message's authenticity is confirmed. Spoofing a hash is virtually impossible, so this tactic offers one way to ensure files and messages weren't tampered with.

Encryption can — and should — happen in a variety of ways in a variety of situations. Windows BitLocker drive encryption is an example of one essentially free solution in the consumer space. Other times, certain hardware may be handy for encrypting data without the need for separate software. Such "self-encrypting" hardware options exist for large hard drives as well as portable flash drives. Web traffic can be encrypted using SSL (Secure Socket Layer), and the list goes on. Simply put, if desired, diligent users can keep their data encrypted wherever it goes.

care providers should go further, particularly with at-rest data on removable storage. One might assume that a portable hard drive or USB flash drive will never be left unattended, but that's precisely the kind of employee wishful thinking and negligence that leads to breaches. Healthcare providers must address this potential weakness.

A Healthy Plan for Healthcare Encryption

Although HIPAA's goal of protecting private patient information remains constant and needed, the legislation became law almost 20 years ago, a time when the environment for electronically stored and transmitted information was quite different from today. For our purposes here, we'll focus primarily on HIPAA's coverage of electronic protected health information (ePHI) and how providers must handle it.

The Security Rule within HIPAA does not explicitly require encryption, but further explanation translates that "no" to "well…basically, yes." Encryption is deemed "addressable," which isn't the same as "required," but the Security Rule goes on to state that entities should perform a risk assessment and implement encryption if the assessment indicates that encryption would be a "reasonable and appropriate" safeguard. If an entity decides not to encrypt ePHI, it has to document and justify that decision and then implement an "equivalent alternative measure."

This spotlights the juncture where industry-standard best practices play such an important role. Similarly, when determining the ideal method of encryption, the U.S. Department of Health & Human Services turns to the National Institute of Standards and Technology for recommended encryption practices. HHS and NIST have both produced robust documentation for adhering to HIPAA's Security Rule (see www.hhs.gov/hipaa/for-professionals/security/guidance). NIST Special Publication 800-111 takes a broad approach to encryption on end-user devices, but in a nutshell it states that when there's even a remote possibility of risk, encryption needs to be in place, and FIPS 140-2, which incorporates the Advanced Encryption Standard (AES) into its protocols, is an ideal choice.

Many organizations leverage the U.S. government's Federal Information Processing Standard Publication 140-2 (FIPS 140-2) to aid in their pursuit of compliance. Specifically, FIPS 140-2 helps healthcare entities ensure that ePHI is "rendered unusable, unreadable, or indecipherable to unauthorized individuals," according to HHS guidelines. A device that meets FIPS 140-2 requirements possesses a cryptographic erase function that "leverages the encryption of target data by enabling sanitization of the target data's encryption key. This leaves only the ciphertext remaining on the media, effectively sanitizing the data."

FIPS 140-2 features four levels of increasing security. Level 1 requires that a solution use an approved algorithm or security function; the device itself requires no physical security. Level 2 adds the requirement for some form of physical security that can present evidence of an unauthorized access attempt, such as a tamper-proof seal. A Level 3 solution goes even further by requiring a countermeasure that thwarts access, use, or modification of the cryptographic module if the solution itself detects a physical breach. Level 4 takes FIPS 140-2 protection to its pinnacle by detecting environmental variations (such as voltage and/or temperature) outside of a specified range and taking action to destroy cryptographic keys when it detects a breach.

Perhaps the best reason to encrypt data came with the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Passed in 2009, the HITECH Act protects healthcare entities from serious penalties for any lost or stolen data provided that the data was encrypted before the breach. Considering examples such as two stolen laptops resulting in a $3 million fine — a fine that could have been avoided under HITECH — the comparative cost of data encryption seems trivial. In other words, healthcare businesses and organizations can't afford not to encrypt all data at rest.

Encryption must extend beyond laptops and backup drives. Communicating or sending data over the Internet needs Transport Layer Security (TLS), a protocol for transmitting data over a network, and AES encryption. When an employee accesses a business's local network, using a secure VPN connection is essential when ePHI is involved. By the same token, before putting a handful of patient files on a flash drive for transfer between systems or offices, a harmless and innocent act in most situations, realize that a self-encrypting flash drive that also meets FIPS 140-2 requirements is the best option to avoid HIPAA violations.

Better Safe Than Very, Very Sorry

Global identity theft losses now amount to billions of dollars. HIPAA violations have and no doubt will result in multi-million-dollar fines and settlements. Protecting sensitive data is more crucial now than ever. If a business or organization within the healthcare industry has questions about securing ePHI, especially when at rest or in movement between locations, a proper risk assessment should be the first step to achieving and/or maintaining compliance.

Encryption will be the correct answer most of the time, but leaving patient data unsecured is the wrong answer every time.

Beyond HIPAA & HITECH: Other Regulations That Matter

Although HIPAA and HITECH compliance should be the first priority for healthcare providers and associated businesses, there are other regulations that may require encryption for data beyond ePHI. Below are a handful of additional regulations likely to apply.

Centers for Medicare & Medicaid Electronic Health Record Incentive Program - Meaningful Use Stage 2 (MU2)

https://www.federalregister.gov/articles/2015/10/16/2015-25595/medicare-and-medicaid-programs-electronic-health-record-incentive-program-stage-3-and-modifications

Now that Stage 2 of the Medicare and Medicaid Electronic Health Record Incentive Programs is in full swing, participants should have encryption and hashing measures in place. MU2 defers to the NIST for appropriate standards to implement.
MU2 links:

http://healthcaresecprivacy.blogspot.com/2012/10/mu2-encryption-and-hashing.html

http://blog.himss.org/2012/09/19/psst-stage-2-meaningful-use-final-rule-impact-to-privacy-and-security/

FDA Title 21 Code of Federal Regulations Part 11 (1997)
https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11
Pharmaceutical manufacturers and others that fall under the jurisdiction of the Food and Drug Administration should be mindful of access to electronic records. Encrypting data at rest and in transit is recommended, and hashing should be used to protect against tampering with data. Title 21 link:

https://www.sans.org/reading-room/whitepapers/analyst/regulations-standards-encryption-applies-34675

Payment Card Industry Data Security Standard (DSS)
Patients' ePHI isn't the only data healthcare providers need to protect. For providers with internal billing departments, handling credit card data — and transmitting it in particular — is subject to the Payment Card Industry DSS.

https://www.sans.org/reading-room/whitepapers/analyst/regulations-standards-encryption-applies-34675

SOURCES

http://www.hhs.gov/hipaa/for-professionals/faq/2001/is-the-use-of-encryption-mandatory-in-the-security-rule/index.html

http://www.4medapproved.com/hitsecurity/hipaa-data-encryption/

http://www.hitechanswers.net/hipaa-doesnt-require-data-encryption-but-you-should/