Why Encryption is Essential in Healthcare Cybersecurity Strategies

ATLANTIC.NET

Secure Cloud Services
Managed & Compliant Infrastructure

888-618-DATA (3282)
sales@atlantic.net
www.atlantic.net

Table of Contents

Throw on any spy movie from years ago and you are guaranteed to get a scene where a code is being written or cracked in some clever manner. While ciphers, lemon juice as invisible ink, and number coding are fun, these methods are easily revealed and used more for entertainment purposes than real security.

So, when an organization needs a reliable, **secure** communication method, what options are available? Encryption is a great answer, but the specifics of that term can be a bit fuzzy. For organizations that have a legal obligation to protect their data from unscrupulous individuals, like those operating in the healthcare industry, it is essential to get their encryption strategy right.

What is Encryption?

Encryption is a way of encoding data so that only authorized parties can receive and understand the information. To successfully encrypt data, an encryption key (a set of mathematical values that both the sender and the recipient have access to) must be available to secure and decrypt the ciphertext upon request.

Generally, encrypted data is referred to as being "at rest" (stored digitally), or "in-transit" (sent through an email or a VPN). Another common term for "in transit" data is "data in use" (data that is subjected to frequent changes as in an operational database).

It is worth noting that **not** all phases of data need to be encrypted, by the letter of the law, but today most are, so it might be more advantageous to adopt this approach from a future-proofing perspective.

Encryption Strategies for "Data at Rest"

Data "at rest" poses a growing concern for businesses and government institutions which have individuals who access this data through mobile devices, which also exposes database management systems and file servers to more risk in the event these devices are lost or stolen.

Encryption best practices typically include methods like AES or RSA:

"The encryption of data at rest should only include strong encryption methods such as AES or RSA. Encrypted data should remain encrypted when access controls such as usernames and passwords fail. Increasing encryption on multiple levels is recommended. Cryptography can be implemented on the database housing the data and on the physical storage where the databases are stored. Data encryption keys should be updated on a regular basis. Encryption keys should be stored separately from the data. Encryption also enables crypto-shredding at the end of the data or hardware lifecycle. Periodic auditing of sensitive data should be part of the policy and should occur on scheduled occurrences. Finally, only store the minimum possible amount of sensitive data."

Already a Standard?

Due to the significant penalties for organizations found to be in non-compliance with HIPAA policies, talking about encryption in healthcare might seem redundant but this is not always the case. Most of us assume that healthcare companies would take the most aggressive approach to data security, smaller providers struggle with HIPAA compliance.

It is easier to empathize with these organizations when one considers the obligations under behemoth pieces of legislation like HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH). Not deploying encryption methods generally does not come from a place of willful malfeasance, but rather a misunderstanding of obligations coupled with small IT teams and budgets.

It is worth noting that encryption implementation specifications in the HIPAA Security Rule is not required and must be based on gap analysis from a HIPAA Risk Assessment. Not all organizations are equipped to perform a proper risk analysis, and as a result, leave protected health information (PHI) exposed to potential cybercriminals.

Taking a realistic look at the industry reveals that most healthcare workers do not get into this line of work to mull over complicated Internet security protocols. Things like encryption might be viewed as obstacles that get between them and providing for patients.

Simply put, executives are put under tremendous strain as they are pressured to adopt electronic health records (EHRs), tasking them with making patient data easier to share while also requiring that data remain safe and secure from unintended recipients.

Be Proactive, Not Overly Complicated

There have been plenty of high-profile data breaches in the healthcare industry over the past five years. Without getting into the nuance of each situation, the result has been hundreds of millions of patient records being compromised and potentially sold on the dark web. The Anthem incident in 2015 is just one example.

For executives, the perceived hassle required to set up, use, and maintain encryption can be unattractive and expensive. For healthcare workers, thinking about encryption might conjure images of complicated health portal systems or clunky services that get in the way to providing patient care.

But taking an approach to HIPAA and HITECH compliance does not have to be overly expensive or burdensome to use. Partnering with technology vendors that

have encryption and turn-key solutions built into their services is the fastest route to compliance and ensuring PHI does not fall into the wrong hands.

What to Look For

Even if a vendor claims to have all their bases covered, it is still important to have a general idea of what that means. Regarding technical safeguards as they relate to encryption, it is important to consider recommended and mandatory encryption protocols, and what would suit the needs of a specific organization.

This is explained in more detail below:

*"**Network encryption** – Encrypt any ePHI to meet NIST cryptographic standards any time it is transmitted over an external network. (Mandatory)"*

*"**Encrypt devices** – All end-point devices that access the system should be able to encrypt and decrypt data, this is particularly important for mobile and laptop devices. (Recommended)"*

Another important aspect to consider is the importance of encrypting employee laptops to ensure no PHI is compromised if the device is stolen.

During COVID-19 more healthcare professionals have adopted a work-from-home model, which presents more threat vectors for those using an unsecured, unencrypted network. Proactive HR and technology teams should work together with vendors to provide robust work-from-home policies to ensure patient data remains secure and encrypted.

For both encrypted storage and a VPN, contact Atlantic.Net and we will be happy to put together a HIPAA-compliant solution for you.

Ready to get started with securing your cloud services?

Contact Atlantic.Net's cloud security experts today about how we can help secure your cloud infrastructure! Reach out to our sales team at **888-618-DATA (3282)** or email us at **sales@atlantic.net**!