Why Isn't Everyone Using Encryption in Health Care?

By Editorial Team | Encryption | Healthcare

Of all industries doing their due diligence to protect sensitive data, you would think that healthcare would be the most vigilant. After all, health data — from cholesterol labs to STD screenings — is about as sensitive and personal as data gets. And on top of normal data security concerns, healthcare providers and administrators also must abide by the Health Insurance Portability and Accountability Act (HIPAA), which piles its own fines on top of providers hit by data breaches. So how safe are patients, really?

has failed to protect its patients: a reluctance to adopt strong encryption in healthcare. While Anthem did use encryption to protect some data, the data that was stolen in the February breach was not encrypted, leading to the leak of 80 million social security numbers. Had Anthem used encryption, it's likely that their customers could have avoided what will most likely be a lifelong struggle against identity theft.

Yet, if encryption in healthcare is such a necessity, why does it seem like so many doctors, insurance companies, and even hospitals are lagging behind?

Smaller Providers Struggle With HIPAA Compliance Uncertainties

most pieces of legislation, HIPAA and Health Information Technology for Economic and al Health Act (HITECH) aren't exactly the easiest things to understand. While technically er piece of legislation explicitly requires encryption in healthcare by default, they do require cal personnel to do a reasonable amount to safeguard protected health information (PHI).

Jay Hodes, President of Colington Consulting, explains why this can be such a trap for smaller health providers. "The encryption implementation specification of the HIPAA Security Rule is only addressable and not required. Most providers do not understand that in order to make a determination on whether to encrypt health data it must be based on the gap analysis part of a HIPAA Risk Assessment," Hodes says. "If the risk is significant, a covered entity or business associate must encrypt those transmissions under the addressable implementation specification for encryption. What I see with most small providers is real confusion in interrupting the all the safeguard requirements of the Security Rule, especially the technical safeguards that must be in place."

Hodes emphasizes how difficult it is for smaller providers to comply with HIPAA, noting that they don't have the large IT teams necessary to manage encryption in healthcare. "It's not that smaller providers don't want to comply with all the HIPAA requirements — it's more of not knowing what they are required to do so. It is complicated and confusing," Hodes says.

Smaller providers might know that they have to protect PHI, but they might not know how to properly do that. This becomes even more of a challenge for providers when you consider that

For most providers, encryption in healthcare is just another nuisance that gets between them and their patients. Mike Meikle (@Mike_Meikle), a partner at SecureHIM, a healthcare security, consulting, and education company, discussed what he sees as a cultural problem in the industry:

> "One must understand that the healthcare business and management model has been very resistant to change. This has been in part due to the incorrect application of market forces to healthcare [illegible] the general workplace culture driven by senior management. [illegible]rmation Technology and Cybersecurity risks are generally not [illegible]n much credence in the executive suite due to more pressing issues taking precedence (reimbursement and revenue cycles, for example). Data encryption, a technology solution, falls far below most executive priority lists."

While patients would like to believe providers are eager to adopt encryption in healthcare, the simple reality is that business executives and health providers aren't security experts. While executives understand how a data leak could impact their bottom line and reputation, they are often willing to roll the dice, much like was the case with Anthem.

On top of that, maintaining HIPAA compliance isn't the only technological challenge that medical practices face. "The failure rate of EMR implementations is high and quite a few healthcare organizations, from small practices to large institutions have had to rip and replace EMRs more than once to address usage issues," he says. On top of that, executives also have to deal with the transition of ICD-9 to ICD-10, which is a diagnostic tool used to help doctors treat patients. "These two large scale projects has all but stolen the attention of executive and board leadership at healthcare organizations," Meikle says.

McMullin also noted that many companies take an "it won't happen to me" mentality. Even though they see other practices completely wiped out because of HIPAA fines, they still believe that they are too small to be a target. As important as encryption in healthcare might seem, these businesses erroneously believe they can sneak under the radar due to their size.

Encryption in Healthcare is Seen as Difficult and Time-consuming

In the eyes of most individuals, encryption is something that's a hassle to setup, use, and maintain. For healthcare executives and workers, encryption in healthcare is just another frustrating hassle. Small healthcare providers hear "encryption" and immediately think of complicated health portal systems, or data encryption services that are clunky and get in the way of their workflow. That's to say nothing of cost, which scares many small providers away from adopting encryption.

For larger institutions that might have the budget to deploy robust encryption systems, the idea of having to train hundreds of employees (not to mention the additional manpower that is needed to maintain such a massive system) is enough to scare them away from using encryption.

"Healthcare providers grow quickly frustrated with multiple logins, authentication regimes, incorrectly applied encryption and general usability issues. Executives hear their doctors complain about encryption issues and make the decision to either pull the products or hobble them in such a way that it negates most of the product's benefits," says Mike Meikle. Even when they are aware of the risks, if executives hear doctors complaining about the system, they likely won't keep it for long."

While no industry thrives on wasted time, there's no space in the medical field for technology that prevents doctors from doing their job. Even if there was a theoretical piece of software that could 100% guarantee that PHI would never fall into the wrong hands, if that system prevented doctors from working efficiently, it would be immediately rejected.

Encouraging Medical Professionals to use Encryption in Healthcare

Luckily, there is an encryption solution that exists that is both strong and easy to use: Virtru. Unlike most solutions on the market, Virtru is designed to be easy to use from the ground up. For encryption in healthcare to work, it has to be seamlessly integrated into the workflow of everyone handling PHI.

Virtru works via a plugin that is compatible with all major browsers and email clients, meaning that there's no need for complicated software or hardware – just download the plugin, and you're good to go. Virtru even works with Gmail, and Outlook, meaning that there's no need for providers to ditch their current email addresses.

uses strong, client-side encryption, meaning that your data is secure from the time you it to the time it is received. Likewise, since Virtru manages your keys, the chance that an ker could gain access to your credentials (and then beat your encryption) is greatly ated.

Interested in seeing just how easy it is to adopt true client-side encryption? Download Virtru today, and enjoy the security of knowing every email you send is protected from intruders.

RELATED POSTS

ITAR Compliance and Email Encryption: What You Need to Know

Protect Patient Data: A Look at Health Data Security and Privacy

Compliance

Digital Workplace

Email Security

+ View All Topics

Dive Deeper

Checklist

ITAR Compliance Checklist for Data Protection

CCPA Compliance Checklist

Data Sheet

Protect Technical Data and Support ITAR Compliance

Products

Gmail Encryption

Google Drive Encryption

Microsoft Email Encryption

Enterprise Apps Encryption

Data Loss Prevention

Audit and Control

Encryption Key Management

Industries

Education

Finance

IT and Software

Government

Healthcare

Manufacturing

Compliance

HIPAA Compliance

FERPA Compliance

GDPR Compliance

CCPA Compliance

ITAR Compliance

NIST Compliance

Company

About Us

Leadership & Investors

Regulatory Compliance

Contact Us

Support

Sales

Report a Vulnerability