4 Critical Questions that Healthcare IT Leaders Need to Ask Themselves About Data Security

What You Need to Overcome HIPAA Security Challenges and Keep Your PHI Secure

The Search for PHI Protection Continues

Healthcare organizations of all sizes are looking for ways to keep patients' protected health information (PHI) secure and private, so they can stay in compliance with the Health Insurance Portability and Accountability Act (HIPAA). A wide range of use cases prompt their search for data security solutions, such as:

- Compliance Officers' concerns over healthcare data sharing between doctors and patients
- IT Managers' requirements for a safer way to send referrals
- Operations Officers' demands for Human Resources staff to securely share and store PHI

These scenarios are increasing organizations' HIPAA compliance risks — and putting IT leaders in a bind. They are especially concerned if they've already tried and failed using different methods for keeping patients' PHI secure and private — from educating employees about HIPAA policies to investing in

encryption portals and other security infrastructure. Even many of today's large data security measures are falling short of data security and compliance goals.

As a result, a surprisingly large number of healthcare organizations are still struggling to overcome their ongoing healthcare information security challenges. They all want something better, something more reliable, and, ideally, something that solves not just their immediate data protection problems, but potential future problems as well.

One way to get to the bottom of their data security challenges and finally find the solution that works is to explore the issues at a deeper level — starting with answering these four critical patient data security and compliance questions.

1. What Kinds of Sensitive Data Do Our Staff Members Handle?

If IT leaders ask themselves what kinds of PHI people in their organization handle in every use case, they'll quickly realize that many categories of PHI are being shared across more scenarios than they initially anticipated. While it might be easy to create a security solution for a single data-sharing use case, solving for multiple scenarios presents more complexity.

For example, if a healthcare organization's IT leadership realized that they were exposing patients' PHI every time they emailed electronic health records (EHRs) to third-parties outside of the organization, such as out-of-network physicians or insurance companies, they could install encryption for that use case and train the HR team on how to use the technology.

It seems simple, right? But what about the HR staff members' other daily data-sharing activities, such as informing a manager that a staff member is having surgery, or emailing employees to request updates to their medical histories. These types of communications and many others fall under HIPAA regulation guidelines, because they all contain private health information. In fact, any health-related communication that identifies someone — including names, addresses, or phone numbers — is subject to HIPAA when used in a medical context. As a result, use cases quickly expand into dozens or even hundreds throughout the organization.

What's Needed?

Healthcare organizations need a solution that keeps PHI secure and compliant in multiple scenarios across an organization. The good news is that with the right solution, it's not much harder to implement an information data security program for three users than it is for three dozen.

2. How Do We Secure Healthcare Data Now?

There are a handful of methods that organizations are currently using to secure PHI, but email encryption portals are the most common. Unfortunately, encryption portals fall short of meeting today's needs for absolute security for all health data.

Encryption portal applications allow users to send and receive information fairly securely. Often paired with Secure Email Gateways and integrated Data Loss Prevention, encryption portals use Transport Layer Security (TLS) to protect the channel where PHI is shared. But the simple idea comes with complex issues. For example, they are not user friendly, especially for external recipients, who need to set up a new account, create and manage another password, and access the protected email in a separate application. As a result, staff and doctors resist using them. Even worse, protecting PHI with basic TLS encryption only secures the communication channel — not the PHI itself. This means PHI can still be breached.

What's Needed?

Organizations need an easy solution for employees to do their part to keep PHI secure and compliant that doesn't require new accounts, credentials, or authentication workflows, doesn't limit secure communication, and doesn't require complex installation and training processes. A better solution is an application that errs on the side of caution by encrypting any data that might fall under HIPAA compliance guidelines. Not only will this meet current needs, but also it will help organizations scale up to address future healthcare information security use cases.

3. How Do We Force Workers to Protect Healthcare Data?

Without a way to enforce data security rules, an accidental healthcare data security incident is almost inevitable. However, most organizations lack the controls needed to enforce HIPAA compliance, or even the visibility to spot a worker breaking the rules. All they can do is raise awareness of HIPAA policies,

provide training and tools for PHI sharing workflows, and hope for the best. But workers have a lot on their minds and years of executing habitual work processes. It's hard to get them to comply with new procedures, especially if they are complex. As a result, often the first time management hears of a data security problem is after there's been a compliance issue or breach. By then, of course, it's too late.

What's Needed?

Healthcare organizations need an application that makes it easy for employees to do their part to keep PHI secure and compliant and gives them the convenience of seamless data encryption. Ease of use significantly boosts adoption and avoids the pushback that comes with complex, inconvenient healthcare information security tools.

4. What Can We Do Once PHI Has Already Been Shared?

This is the question that keeps IT leaders up at night. We've all made a few email mistakes, such as typing the wrong address or accidentally hitting "Reply All." Typically the consequences aren't any worse than mild embarrassment. But the embarrassment can turn into HIPAA noncompliance if, for example, that accidental email contains a patient's health data, such as a diagnosis or a test result. That one innocent mistake could result in costly HIPAA penalties, stressful audits, and onerous disclosure and remediation plans.

What's Needed?

Organizations need an encryption tool that lets them immediately undo their email mistakes by revoking access to PHI — even if recipients have already opened the email or files. Further, if the program provided "read receipt" functionality, the organization can identify exactly who has read the message and who hasn't. Then they can conduct remediation with the recipients who had accidently read the email contents, a step that will help them remain in compliance.

Virtru — Making It Easy to Protect Healthcare Data and Share It With Confidence

Secure PHI is the Holy Grail of today's healthcare world. But, despite years of searching for the right security solution, organizations still struggle — and healthcare remains the most breached industry. With today's stricter HIPAA rules and more costly fines, it's time for organizations to finally solve this

chronic problem. One solution was designed specifically to overcome all of these challenges and deliver exactly what the industry needs to lock down PHI — Virtru.

Virtru delivers a level of data security that existing solutions can't. Secure, easy-to-use data-sharing capabilities include:

- **Familiar Workflows**. Works with your existing applications and workflow — versus forcing your organization to adopt new processes, and forcing users to create new accounts and additional logins.
- **User Adoption**. Boosts adoption with industry-leading usability that keeps user engaged—versus complex user experiences that encourage workarounds.
- **Automatic Protection and User Warnings**. Enables customizable rules to enforce protection and warn users by scanning email and attachments for keywords, social security numbers, medical codes, email addresses, and other PHI.
- **Access Controls**. Enables access controls to disable forwarding, set expiration dates, and watermark attachments to prevent data leaks.
- **Email Recall**. Supports email recall with a single click — revoking access and preventing recipients from reading or forwarding it in the future.
- **Visibility** Delivers read receipts and granular tracking on who's seen what, when, and where, which supports compliance audits.

Future Focus. Addresses future healthcare information security use cases and by keeping PHI protected throughout the patient's entire course of care.

See Virtru in Action!

Request a live demo today.