ipswitch

Secure. Control. Perform.

AN IPSWITCH SECURITY GUIDE

IT Challenges and Solutions for Protecting Healthcare Data

ipswitch

Introduction

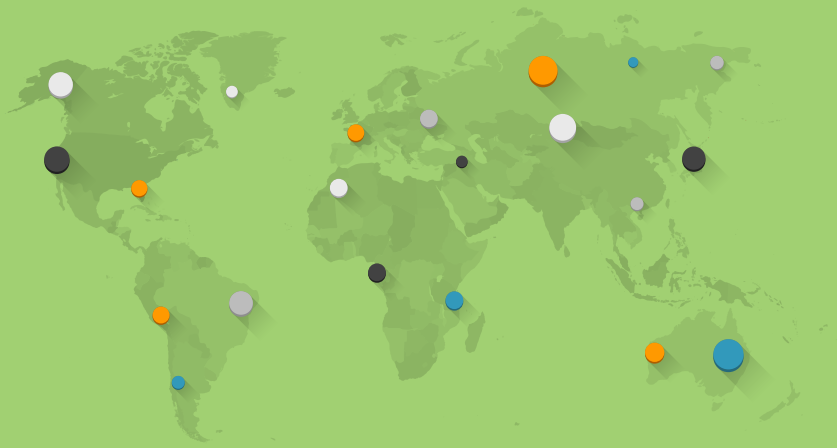
Not all that long ago the healthcare industry finally embraced the information age, thanks to the widespread adoption of toolsets such as those from Epic Systems and MEDITECH. Electronic health records (EHRs) make critical healthcare information available exactly when and where it is needed. Handwritten notes and idiosyncratic filing systems have largely become things of the past.

Even though digital healthcare information provides huge benefits, it also presents huge challenges because this all-important data needs to be secured through data encryption. And it's not a simple task to lock down healthcare data in motion and at rest.

Even though handwritten notes and medical records could be misplaced (or deemed unreadable) when needed most, at least they couldn't be hacked. On the flip side, EHRs can be hacked, and are really attractive to cyber criminals because they are worth more than a stolen credit card number.

NEW POSSIBILITIES

When all medical information lives in one place and accessible by any authorized healthcare practitioner, a lot more can be learned through big data analytics. Tracking the Zika virus from its roots in South America to other parts of the world is a compelling example of the power of correlated data to provide healthcare insights.



ipswitch

In this eBook, you will learn about:

- The evolution of healthcare data
- Why healthcare data is so attractive to hackers
- The challenge of data security
- End-to-end encryption solutions
- How Rochester Regional Healthcare uses managed file transfer (MFT) to secure patient data and meet regulations

From Small Towns to Big Data

Back in the day, medical information was a lot less fragmented. People stayed put in their home towns. Physicians made house calls. Patients changed doctors only when theirs retired. There were far fewer specialists and medications. Labs results as we know them didn't exist yet.

As medical science advanced through research and patient treatment, the need for reliable healthcare data dramatically increased. Fast forward to the present and technology resources provided by EHR software provide the backbone for information flow throughout a healthcare organization.

Healthcare technology like imaging systems and advancements in medicine have increased the quality of patient care and the cost to keep people healthy. To maximize revenue, healthcare practitioners are expected to see as many patients as possible in one day. This leaves little time to waste tracking down medical records or dealing with archaic systems that keep them filed away.

The evolution of healthcare technology has not only resulted in better patient care but also the ability to make data correlations and identify patterns in a way not possible before. When all medical information lives in one place and accessible by any authorized healthcare practitioner, a lot more can be learned through big data analytics. Tracking the Zika virus from its roots in South America to other parts of the world is a compelling example of the power of correlated data to provide healthcare insights.

ipswitch

One Hundred Times More Valuable Than Stolen Credit Cards

What can be hacked usually gets hacked — especially if there is money in it. Personal health information (PHI) is a gold mine of personal data and a big target. According to James Scott of the Institute for Critical Infrastructure Technology (ICIT), personal health information is one-hundred times more valuable than stolen credit cards. Abuses of PHI range from peddling fake miracle cures to desperate patients to outright criminal activity like blackmail or ransomware infections. Attacks are happening on a weekly basis.

On top of that, adds security expert Avi Rubin, the healthcare industry is the "absolute worst" when it comes to cybersecurity. Medical professionals are trained to worry about saving lives, not protecting sensitive information. And the same factors that made the healthcare sector slow to go online — its fragmented structure, and the simple fact that so much of medical professionals' work is done on their feet in hospitals and clinics, not at a desk — makes security protections and procedures harder to implement.

It's no surprise that hackers have found the vulnerabilities in healthcare IT and are attacking healthcare data systems at increasing rates, with increasing success. In March 2016, 21st Century Oncology reported a data breach affecting 2,213,597 individuals, according to the U.S. Office of Civil Rights. Just a few months later PCWorld reported that a hacker claiming to have stolen 9.3 million records from an unnamed health insurance provider had put the records up for sale on the dark web for about $850,000.

The Challenge of Data Security and Encryption

Securing sensitive data is never easy, especially in a fluid environment. A survey conducted by Freeform Dynamics in association with Ipswitch, showed that nearly three quarters of professionals rated their organization's ability to handle document and file transfer security as either "needs strengthening" or "already inadequate."

There are basically two ways to keep data out of the hands of hackers. One is to protect every endpoint leading to it, making it essentially inaccessible. The other is to encrypt the data, so that even if hackers get to the document they cannot read it. In addition, sensitive data should be backed up daily in case of ransomware.

End-to-end encryption that covers both data at rest and in motion offers the best protection to a document throughout its lifecycle.

Most ransomware attacks end with healthcare companies dishing out tens of thousands of dollars' worth of bitcoins to cyber criminals. In the unfortunate event that you do come under attack, a recent backup will allow you to quickly resume operations with minimal impact, assuming the ransomware isn't present in the backup.

These protective approaches can and should be used. But given the tough operational environment that medical professionals work in, healthcare data encryption is, by a wide margin, the single most powerful tool for safeguarding confidential PHI.

End-to-end encryption that covers both data at rest and in motion offers the best protection to a document throughout its lifecycle. And because the encryption process can be automated, it can be deployed with confidence, even for those who are not accustomed to applied security.

End-to-end Encryption Solutions

Where simple file transfer protocol (FTP) was once sufficient, today IT has to reach for more capable and secure infrastructure that mixes the end-user simplicity of Enterprise File Synchronization and Sharing (EFSS) like Dropbox with the reliability of FTP like WS_FTP. They need to do this in a way that doesn't inadvertently make what has traditionally been a solvable problem into a messy custom development situation.

This is where managed file transfer (MFT) fits in. MFT is a purpose-specific class of middleware focused on the reliable transfer of files between business parties, using simple, secure protocols and easy-to-understand models of exchange. It's fortified with secure encryption, manageability, scalability, file processing, integration, and business-reporting options that allow IT to deliver more sophisticated, controlled file-transfer solutions without slipping into the custom-code abyss.

ROCHESTER REGIONALHEALTH

"Different people from different organizations are getting access to the tool, and the central security model lets you delegate tasks to certain groups of people, and that's really helping us out there."

Dylan Taft, Systems Engineer

How Rochester Regional Healthcare Uses Managed File Transfer to Comply with Strict Regulatory Requirements

Rochester Regional Healthcare has more than 15,000 employees throughout eight affiliate locations. Its primary facility, Rochester General Hospital, sees more than one million outpatients annually. The IT team at Rochester regularly needs to transfer data between locations and partners. For example, the billing department regularly exchanges patient records and claims with healthcare providers, payer organizations and insurance companies. These records must be secure, manageable and easy to access.

Dylan Taft, systems engineer for Rochester Regional Healthcare, was tasked with finding a file transfer solution to solve the mounting problems created by an existing patchwork of scripts and servers. He knew they needed something to manage the high amount of file transfers while maintaining HIPAA and HITECH compliance and improving security. Dylan also knew the right solution would allow for secure integration with the growing number of cloud-based apps making their way into healthcare industry.

As a result of the existing homegrown file transfer method, the IT team at Rochester Regional Healthcare faced these particular challenges:

- A lack of centralized monitoring and documentation of data transfers
- A need to securely exchange data with new cloud applications
- A requirement to maintain compliance standards and internal security protocols

Dylan set out to modernize his file transfer system and came across Ipswitch's automated file transfer solution, MOVEit. The search ended there; high security levels, ease of implementation and app integration made MOVEit the clear choice.

Once MOVEit was in place, Dylan and his team had the tools to make some innovative changes, including:

- A central access point for control and visibility that spanned throughout the organization, affiliates, payer systems, insurance companies and all integrated applications
- A standard method for users to create and manage tasks in one central location
- Automated secure data transfer with cloud applications
- Quickly trained new employees to use MOVEit

Each of these new innovations maintained compliance with HIPAA and HITECH regulations and improved overall security.

Data Security is a Neverending and Thankless Job

The responsibility for safeguarding sensitive company information and securely transferring it falls on the already stretched thin IT departments. Luckily, there are many options available for IT when it comes to file transfer. Email, FTP, USB drives and EFSS services like Dropbox to name more than a few. Yet none is as secure or cost-effective as managed file transfer.

MFT gives IT teams the agility they need to respond faster to business needs while reducing time and resources required for file transfer operations.

About Ipswitch

Ipswitch helps solve complex IT problems with simple solutions. The company's software is trusted by millions of people worldwide to transfer files between systems, business partners and customers; and to monitor networks, applications and servers. Ipswitch was founded in 1991 and is based in Lexington, Massachusetts with offices throughout the U.S., Europe and Asia.

For more information, visit **www.ipswitch.com**.

ipswitch

Download your 30-Day FREE TRIAL of Ipswitch MOVEit ›