7 File Transfer Challenges of Healthcare IT Teams

ipswitch

ipswitch

Introduction

The digital evolution taking place in healthcare organizations is resulting in an explosion of easily accessible data relating to patient care. Healthcare organizations are becoming acutely aware of the security risks presented by this data in the form of misuse, theft or ransom attacks.

Much of this data is also within the scope of Personal Information Protection Acts (PIPAs) in force in over 25 countries including regulations such as the EU's General Data Protection Regulation (GDPR) and the Australian Data Privacy Acts. These data protection regulations seek to minimize the risk of privacy loss to patients by establishing stringent standards for protecting personal data. There are numerous, recent examples of enormous fines levied against healthcare organizations found in violation of these regulations.

Often overlooked, are the significant risks involved in the healthcare business processes that require the external exchange of sensitive and personal data. Today's healthcare organizations are often relying on outdated legacy systems which were not designed with data protection regulations in mind.

Make no mistake: the automated, integrated movement of files is the crux of the matter. And as we'll see, "business as usual" FTP and e-mail file transfer systems just aren't adequate anymore.

Drop-box-like solutions aren't the answer either, since they're designed for file sharing, not file transfer. As patient services grow in scope, to include things like appointment reminder services and satisfaction surveys, so do the risks of external data sharing.

EXTERNALLY SHARING SENSITIVE PERSONAL DATA?

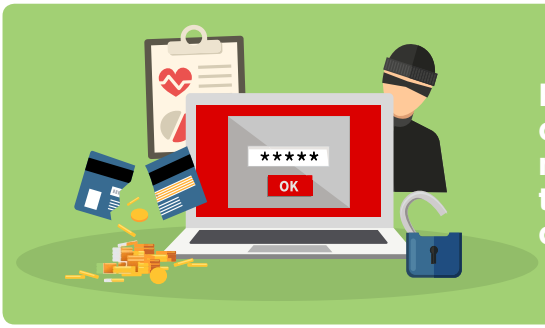
Exchanging medical records with external sources for payer reimbursements or eligibility queries is a necessary business process. It is also, however, most likely within the scope of data protection regulations such as the Personal Information Protection Acts (PIPA) of several countries or the Australian Data Privacy Acts.

Many of these acts require safeguards that surpass the security and compliance features of typical EFSS or FTP solutions.

ipswitch

There are legacy productivity and process problems, too. Ask yourself these important questions:

- Has there been a significant increase in the sheer volume of confidential patient files your systems are handling? How about the complexity of the files?
- Is the challenge compounded by the use of cumbersome DOS scripts?
- Even though your tasks may be "automated" batch jobs, is the scripting for file transfer job creation and execution proving to be time consuming and error prone? Do these scripts enable the activity logs that will be required in an audit?
- Do you have difficulty determining when a file was transferred, where it went, and if it even got there? Do you sometimes have to spend hours or days searching?
- At times, is the scheduling of file transfer jobs a monumental challenge (for example, manually rescheduling every job when a password changes)?
- Do your end users sometimes circumvent IT and use unauthorized file transfer solutions that put confidential claims data, pharmacy records and patient information at risk?
- Given these everyday challenges, do you feel you're already playing "catch up" when it comes to implementing the measures that may be required by applicable data protection laws?



Personal Information (PI) drives a thriving black market for cybercriminal tools, expertise and stolen data.

ipswitch

Zero visibility with file transfers is a bad way to start your IT day.

You know the drill. You spend the first 90 minutes of the day staring at your screen like a zombie, trying to make sense of the errors, exceptions and problems that greet you every morning. This can often involve the futile task of trying to track file transfers as you seek to answer questions such as what clinical data was sent, where was it sent, was it received, and when and how did it get there? And right now, this very minute, what is the real-time status?

Think of the time and effort this can cost you—and how you can sometimes come up empty-handed. The problem is you have no visibility, or very little of it. Or you have to painfully pore through detailed log reports to find what you're looking for. You simply don't have the tools to monitor, manage and audit the transfer trail of files across your enterprise—a failing that means your supposedly "okay for now" file transfer solution is really woefully inadequate. And robust reporting capabilities? A dream, at best.

Your job is hard enough without having to contend with these blind spots and drawbacks. But things can definitely get worse—much worse—when the lack of visibility has security and compliance implications...

Everyone's demanding security and compliance.

Your Security, Compliance and IT teams design and manage processes that ensure the security of protected data. The regulators oversee your stewardship of this data as they enforce the laws. But then...an over-eager end-user who insists on an "easy, fast" workaround makes a poor choice of storage or transmission of personal data that leads to security being compromised.

You're the one who's asked to fix the problem. And what a problem it is. If you can't produce the right files at the right time, or if you can't prove they were properly protected, your organization could be subject to tens of millions in government fines and penalties, a battered reputation in the healthcare community, and a loss of trust by medical professionals, patients, and the public at large.

ipswitch

Stakeholder requests never seem to end.

Ever wonder if your workload is really getting heavier, or if it just seems that way? Well, it is getting heavier. A quick look at a few statistics bears this out. According to a recent Aberdeen study, the volume of file transfers is increasing, on a yearly average, by 11%; the size of files by 7%, and the number of users transferring files by 6-9%. All while IT hiring goes up by a paltry 2%.

Those averages are across all industries. Needless to say, certain healthcare organizations are seeing an escalation in file transfer demand that is even more extreme.

Lack of integration and centralization can be serious liabilities.

It's easy to get used to a lack of a centralized, unified solution set for file transfer. But it's never acceptable. It's inefficient, chaotic and needlessly confusing. You can feel like you're running in an endless maze.

Of course, it's not like your file transfer systems were created this way by design. It's the way initial systems were developed and introduced one at a time—one system in radiology, for example, and another one in obstetrics— with lots of home-grown improvisation and "band-aid" fixes along the way.

Needless to say, this cobbled-together patchwork is not the best way to ensure trouble-free file transfers that minimize the risk of disappearing files and exposed records. Instead, it would be far preferable if you could find a solution that consolidated file transfers into a single system across doctors, nurses, administrators, partners, applications and systems—enabling you to ensure fewer points of failure and guarantee simpler integration efforts.

ipswitch

5 It's time to say goodbye to "good old" FTP and e-mail file transfers.

These solutions feel like old friends. They've most likely been around your organization for quite a while—and you, and your end users, know them quite well. But they just don't provide the security you need to comply with today's regulations. Here are some examples of their shortfalls:

E-MAIL FILE TRANSFERS

- Data is not encrypted in transfer.
- No visibility as to where files are—either for you or an auditor.

FTP

- Even with SFTP or FTPS, files are still often left exposed and unencrypted on the FTP server.
- Integration with your security infrastructure and authentication systems is often lacking.
- Multiple servers limit your ability to centrally control and provide an audit trail for sensitive data transfers.

DROP-BOX LIKE SOLUTIONS

- These are file sharing solutions, not necessarily file transfer solutions. They're designed for collaboration, but do not have the management and infrastructure to facilitate file movement as a part of business processes.
- Built on lightweight infrastructure that often can't support enterprise level requirements for security, audit-ability, reliability and visibility.
- For some businesses and processes, the additional layer of storage management and administration is a hassle and unwanted expense.

ipswitch

Your productivity is being hurt by complex manual processes and a lack of automation— and did we mention custom scripting?!

Here's a continuation of the previous point. It comes down to the fact that you're probably compensating for your organization's lack of automation by devoting countless hours to complex manual file transfer tasks, laboriously writing code every time there's a change to business processes, and performing repetitive, tedious jobs such as partner on-boarding, and managing data and file exchange with partners.

All of these responsibilities can chew up large chunks of your day. Chances are, they're the reasons your mission-critical file transfers are taking way too much time—to the dismay of just about everyone in your organization. And you can't really blame end users for being upset by the delays and calling you for clarification and updates—it's ultimately the health and well-being of patients that are being put at risk.

When end users go around you, it's like they're taking aim right between your eyes.

It's guaranteed: When there's no centralized, IT managed file transfer solution, your end users will turn to whatever tool offers them the greatest convenience. The downside is that convenience comes with a price—namely, an increased risk of security breaches and non-compliance. Furthermore, with the proliferation of mobile devices, the possibility of porous, easily-compromised security is magnified all the more.

What's needed, then, is a unified standard for all file transfers in your organization—an easy-to-use solution that integrates seamlessly with the tools your end users are already employing. But where do you find such a solution?

ipswitch

FEWER ERRORS. FASTER RESOLUTION

Research indicates that organizations that adopt MFT have, on average, 26% fewer errors, exceptions and problems with file movements, and resolve the errors 4.8 times faster than those that do not.* Very impressive figures—and all the more reasons to take decisive action.

** Move Away from the Tangled, Digital "Do-It-Yourself" Approach to Moving Files:* Aberdeen Group Webinar, December 2013

Managed File Transfer (MFT) enables regulatory compliance and mitigates data security risks.

You're not alone in the challenges you face as you seek to maximize the effectiveness of your file transfer systems—and to meet government compliance regulations. Many other IT professionals in the healthcare industry are facing similar challenges and share in the pains you're experiencing.

The good news is that there is a solution—an enterprise-class Managed File Transfer (MFT) system—which allows you to meet your growing (and increasingly complex) file transfer needs. It can be delivered to your doorstep neatly and simply. And it enables you to transfer files reliably and securely, meet your all-important compliance requirements, eliminate manual workflows, and provide end users with an IT-approved solution for sending files. MFT also guarantees you visibility and control over all file transfer activities, enables you to confidently meet your SLAs, and provides you with easy implementation/on-boarding.

Specifically, with MOVEit® MFT Complete from Ipswitch File Transfer, you'll receive four vital benefits that are unavailable with the all-too-common array of legacy systems:

- **Accessibility** ensures that end users can access the system via mobile devices, email, or a web browser. Easy-to-use interfaces help assure that user-based ad-hoc data transfers are secure and compliant.
- **Administration** so that you can easily set up, control, and manage your organizational file transfers, provision users/accounts easily, and on-board partners and control access.
- **Automation** to make sure that files route appropriately according to key business processes and they integrate into other applications for scheduling and routing.
- **Reporting** for enterprise visibility and control, compliance and governance and to easily provide reports for auditing and regulatory inquiries.

How will MOVEit impact you and your organization? For starters, you'll be better able to meet compliance requirements, which greatly reduces pressure on you. You'll increase productivity and efficiency within IT and all across your organization. Costs will be reduced. And the quality of your patient care will be enhanced— thanks to faster, more secure file transfers that are vital to a streamlined workflow and processes that support your entire team of healthcare professionals.

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

Learn more about Ipswitch MOVEit ›