globalscape™
securely connected

Whitepaper

Protecting Digitalized Assets in Healthcare

Which Managed File Transfer (MFT) Deployment Model is Right for You?

In 2011, a Boston-based healthcare provider was fined $1 million by the HHS following a data breach that affected nearly 200 patients. This organization was also forced to take additional steps to reduce the risk of future data breaches, including delivering semi-annual reports verifying the firm's compliance to the HHS for three years.

The digitization of information has had a tremendous influence on organizations in every sector, but most especially on healthcare. Doctors, nurses, clinicians, and other professionals are increasingly relying on digital file sharing solutions and electronic health records (EHRs) to optimize the quality and efficiency of the care they provide.

However, these technologies create tension: While healthcare professionals are eager to leverage digital files to improve productivity, these behaviors can present serious security and compliance risks. Care providers understand that they need to keep patient data secure and compliant, but they won't sacrifice speed and quality of care. If forced to choose between optimal patient care and data protection, the vast majority of healthcare professionals are going to choose the former every time.

The onus is therefore on healthcare IT to implement policies and tools that cater to the new information-sharing needs of today's healthcare providers. By doing so, organizations can enable doctors, nurses, and clinicians to perform their jobs with optimal efficiency and keep patients' sensitive information secure at the same time.

Digitization in Healthcare: The Risks and Rewards

The implementation of EHRs is commonplace among healthcare providers, and will continue to become universal, as mandated. Yet for all of the benefits and advantages offered by EHRs and other digitization efforts, it is critical to note that this trend also presents serious dangers. By making medical histories and other sensitive patient data more accessible, digitization also increases the likelihood that a data breach will occur.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)

For many physicians, access to sensitive patient data—both off-hours and off-location—is necessary to providing optimal care. And while the act is often well-intended, many individuals rely on consumer-grade file sharing options (such as Google Drive, Dropbox, USB devices or personal email) to move sensitive information, which increases the risk that the files may be viewed by unauthorized personnel. The consequences are often severe for an organization, both financially and from a reputation standpoint.

These breaches are far from uncommon. A recent report from the Ponemon Institute found that 94 percent of surveyed healthcare organizations had experienced a data breach within the past two years. In the first quarter of 2013 alone, 875,000 records were exposed via breaches.

A recent report from the Health Information Trust Alliance (HITRUST) determined that there have been nearly **500 data breaches reported to the Department of Health and Human Services (HSS) since September 2009.** A total of 21.1 million records were exposed in these incidents, with an average size of more than 40,000 records each. The cost of these data breaches averaged to more than $8 million per incident.

In addition to the direct costs, these organizations risk severe fines for failure to achieve data security compliance. The Health Insurance Portability and Accountability Act (HIPAA) established standards that healthcare providers must meet when it comes to ensuring the security and privacy of patients' sensitive information. Those organizations that have failed in this duty have faced fines and other sanctions.

Lastly, there are serious indirect costs that emerge in the wake of a breach. Perhaps most notably, breaches undermine patients' trust in healthcare providers. The public is becoming increasingly aware of the potential ramifications that can result for individuals whose personal information has been exposed by an organization, such as identity theft or fraud. If a particular healthcare provider experiences a data breach, its patients may become less willing to share their private information. This lack of trust can put serious strain on the doctor-patient relationship, and adversely affect care outcomes.

Yet many healthcare organizations are not taking sufficient steps to prevent future breaches or minimize the damage of these events. Nearly 40 percent of healthcare providers surveyed by the Ponemon Institute this year indicated they had no data breach response plans in place, and only 19 percent stated that they are equipped with the tools needed to gauge the size and cause of a data breach.

Securing Medical Data

Fortunately, despite all of the dangers and challenges, the fact remains that EHRs and digitization can be tremendously valuable for healthcare providers.

Fortunately, despite all of the dangers and challenges, the fact remains that EHRs and digitization can be tremendously valuable for healthcare providers.

Here are four strategies that healthcare providers should implement to ensure that digital medical records and other sensitive files remain secure and compliant while being sent, received, and accessed by employees:

1. Work Directly with the End Users (Physicians, Nurses and Medical Staff)

Doctors, nurses, and other clinicians face tremendous pressure every day, and won't stand for any policy that holds them back from doing their jobs quickly. For IT, that means understanding the environment in which care providers operate. That is, care providers often need to contact and share information with patients while outside of the organization's secure, managed infrastructure, perhaps while at home or on the road. The task for IT is to make sure that all policies enable productivity and provide tools that cater to the on-demand needs of today's healthcare worker. One of the most damaging mistakes healthcare organizations can make is failing to work directly with the physicians and nurses who handle sensitive data every day.

2. Make Sure Everyone Understands What's at Stake

Education is crucial. Teach your staff about the risk of data breaches. Do they understand the financial ramifications for the organization? Do they understand the negative publicity a data breach creates? Do they understand the risks vs. benefits for the patient?

3. Implement a Secure MFT Solution

Managed file transfer (MFT) is among the best available means for healthcare firms to distribute data securely. A high-quality MFT offering will provide users with the ability to send files—of any size—instantly, and with minimal effort.

This is particularly important considering the current state of the healthcare industry. MFT solutions represent a critical opportunity for healthcare providers to integrate IT security with EHR utilization, which makes medical information more easily accessible and shareable between physicians.

Additionally, MFT tools fuel faster, more efficient exchanges of information between physicians and their patients, improving the quality of care, the doctor-patient relationship and the healthcare provider's ability to comply with EHR meaningful use objectives.

4. Conduct Security Testing

The data security landscape is constantly evolving. Organizations need to regularly conduct tests to ensure that their secure file sharing and other data security systems remain effective and reliable. As circumstances change, such as a significant increase in the number of patients or employees at a given firm, data vulnerabilities may emerge. By periodically stress testing the data management and sharing solutions, healthcare providers can maintain a consistent level of security.

Summary

IT professionals need to provide clinicians with an easy, efficient, secure way to access and share patient records and medical files. While care providers must exercise their own discretion, it's up to IT to provide tools and create policies that foster efficient patient care, security, and compliance.

About Globalscape

Globalscape ensures the reliability of mission-critical operations by securing sensitive data and intellectual property. Globalscape's suite of solutions features Enhanced File Transfer™, the industry-leading enterprise file transfer platform that delivers military-grade security and a customizable solution for achieving best-in-class control and visibility of data in motion or at rest, across multiple locations. Founded in 1996, Globalscape is a leading enterprise solution provider of secure information exchange software and services to thousands of customers, including global enterprises, governments, and small businesses.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)