ShareFile®

CITRIX®

THE TRUTH ABOUT CLOUD SECURITY

13 Facts Your Healthcare Organization Needs to Know

#BetterWayToWork

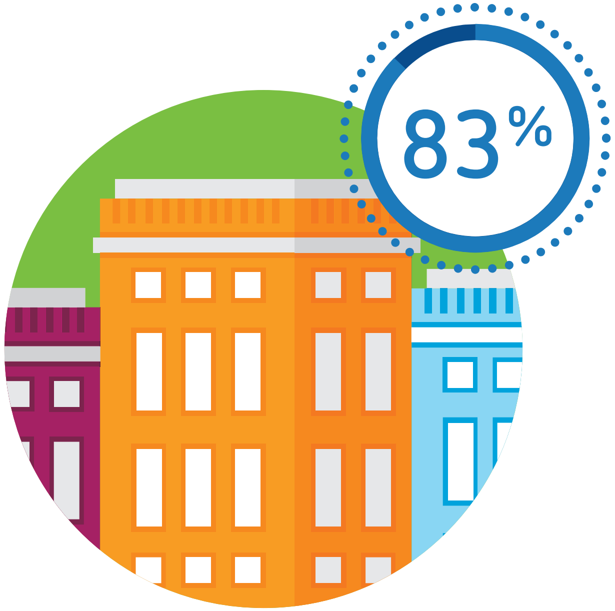
TABLE OF CONTENTS

CLOUD SECURITY: IS IT A PROBLEM?

82 percent of healthcare organizations rated security as their number one concern.

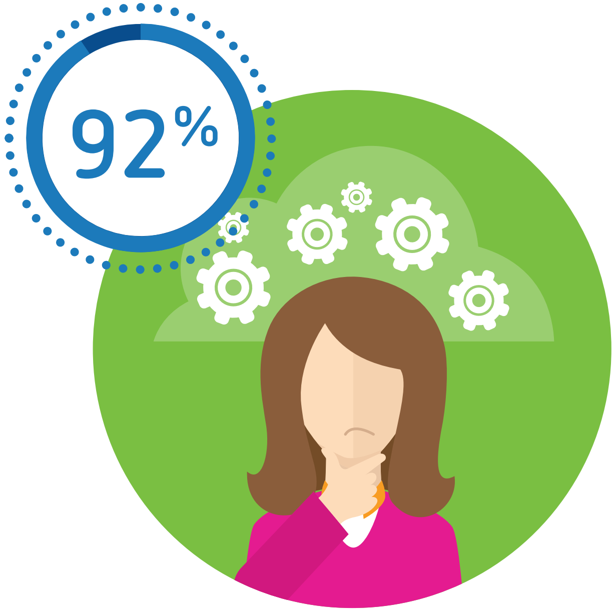
In the healthcare industry, patient privacy is vital. In fact, the Health Insurance Portability and Accountability Act (HIPAA) requires all healthcare practices to ensure the privacy and security of protected health information (PHI) and electronic protected health information (ePHI) around the clock. Even though the technology used to collect, store and share PHI, medical histories, DICOM studies and more has come a long way, many small and medium organizations are uneasy about adopting new cloud-based solutions fearing security risks. But as it turns out, this hesitation to embrace new digital tools may be what's standing between you and more secure, efficient and productive patient care.

Consider these recently published results from HIMSS Analytics:



83 percent

of healthcare providers are using cloud services.



92 percent

said they see the current and future value of cloud services for their organizations.

These numbers paint a fascinating picture: despite the warnings, many medical providers already trust these services with patients' most sensitive data. Additionally, regulatory agencies continue to release recommendations for CPAs to establish secure, practical data governance with online tools. With some due diligence, security and compliance in the cloud is possible, and achievable for your organization.

So what are the real security risks associated with cloud software, and how can you mitigate them?

Let's dig in and get a better understanding of cloud security.

IT ALL STARTS WITH THE INTERNET

It's understandable to be hesitant about putting patient data on the Internet considering it is, essentially, a publicly accessible network, with almost no security for your data built-in. While you might find that risk acceptable for your personal photos and social networking, it's clearly not good enough for the kind of sensitive patient data that healthcare professionals handle on a daily basis. To work around this limitation, business-class cloud services utilize **encryption:**

ENCRYPTION

A technology that transforms data in undecipherable code while it travels between secure destinations that can only be opened with a specific key.

63 percent of healthcare organizations said they were using the public cloud to store data, but **25 percent** of these organizations are still not encrypting their data.

Trying to set up a robust encryption system for your business might be above your skill and comfort level, but there's no need to worry. Look for cloud solutions that encrypt data automatically—giving you security without additional overhead or effort.

ShareFile®

IT'S NOT THE CLOUD ITSELF

While the biggest worry about cloud software can be mitigated with encryption, there are other vulnerabilities your business needs to think about. However, these concerns must to be addressed whether your business is using cloud software or local software tools:

Will your employees keep their login credentials safe?

Will you be able to maintain control over your data?

Will a cloud service provider comply with regulatory standards?

THE MAJOR ISSUES WITH DATA SECURITY

These are valid concerns:

53 percent of IT professionals listed access control as their primary cloud security concern.

Just one-third of businesses considered external data sharing to be their greatest concern.

On the other hand, 79 percent of data security pros consider end users, not the underlying technology, to be their greatest security headache.

UNDERLYING CLOUD SECURITY CONCERNS

If cloud technology is not the main problem with security, then how can your organization mitigate other concerns?

84 percent of businesses

aren't happy with traditional security tools when it comes to safeguarding the cloud.

51 percent

said they are emphasizing internal policies.

49 percent

indicated they are focusing on security visibility.

The cloud has matured to a place where traditional data protection – which puts a spotlight on the technology – is only part of the solution. Your management and governance policies should also be held accountable for their contribution to security efforts.

MOVING PAST PASSWORDS

Access control is one of the major "people problems" that can ruin your day. Poor password practices can drive anybody crazy, but fortunately, modern technology has evolved to make it easier to safeguard your work.

66 percent of workers

said they are using methods beyond just passwords to keep data safe.

91 percent of security professionals

think passwords will be a thing of the past within a decade.

User authentication can be a cloud security hang-up, but modern apps are giving you more options, making it easier to keep data safe without the extra stress of trying to remember dozens of passwords – a single cloud service means remembering a single set of credentials, and could help you improve regulatory compliance as well.

AUTHENTICATION OPTIONS

Cloud security has evolved to give you more options than ever when it comes to protecting personal credentials. A few popular tools include:

Fingerprinting scanning

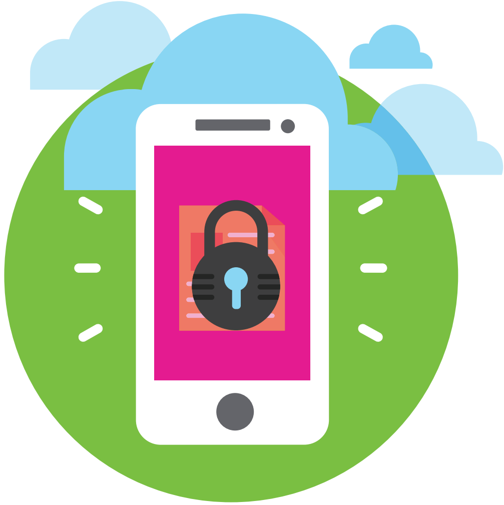
28 percent of the world's smartphones currently have fingerprint scanners. Simple biometrics let you take advantage of multiple points for authentication without sacrificing convenience.

Single sign-on

Identity and access management tools let you use complex passwords or multiple authentication methods without hassle. The identity and access management market will rise at a CAGR of 12.2 percent from 2015 to 2020. Many cloud apps and services are building single sign-on functions into their architecture so you don't have to worry about it.

MOVING CONFIDENTLY INTO THE CLOUD

Many cloud service providers have more resources than your healthcare organization when it comes to security – it's a key part of their job after all. In fact, this is a key point **highlighted by Gartner**, a research firm that specializes in analyzing cutting-edge tech adoption, as a reason to take advantage of the cloud.



User authentication is also evolving as more businesses ramp up cloud deployment. This leaves visibility and policy compliance as key issues, and those are problems that individual apps can handle for you. For example, industry leading collaboration technologies offer built-in document tracking and notifications so you always know who has access to your files and what they're doing with the data.

In the eyes of many healthcare providers, cloud technology has now evolved to become even more secure than other solutions including on-prem. With the right tools, and the right precautions in place, you can rest assured that your sensitive data is protected and focus more quality patient care.

LEARN MORE

It’s not possible to eliminate risk, but you can decrease it significantly by becoming aware of security issues, learning everything you can and being proactive in your responses. With Citrix ShareFile, you can enjoy simple, secure cloud-based file sharing and collaboration that supports compliance.

Visit www.ShareFile.com to learn more.