documo

# 4 Misconceptions Regarding HIPAA Compliance and the Cloud

A White Paper Study

# 4 Misconceptions Regarding HIPAA Compliance and the Cloud

As health professionals, it's essential to take every precaution to protect sensitive patient information including personal contact information and medical history. The government regulates patient data and provides privacy and security provisions for safeguarding medical information. The law that governs these processes, the Health Insurance Portability and Accountability Act (HIPAA), has become a prominent point of public discussion over recent years due to an onslaught of security concerns and cyber attacks on health providers and insurers.

*42% of organizations note a common cyber exposure they face is holding information that is subject to HIPAA (Statista).*

Navigating healthcare data can be confusing, so we have broken down the four most common misconceptions associated with cloud computing and HIPAA compliance. As health offices increasingly turn to cloud solutions to eliminate paper files from offices, securing fax and other technical safeguards are critical. With the proliferation of cloud and mobile computing increasing each year, organizations have little choice but to adapt and must navigate the growing number of service providers that best protect patient data.

## Regulating Cloud Computing & HIPAA

Cloud service providers (CSPs) offer online access to shared resources and provide entry to servers, databases and a broad set of applications across the internet. CSPs also cover solutions relating to HIPAA compliance.

In evaluating whether the cloud solution you are choosing is HIPAA compliant, it's important to understand what exactly HIPAA compliance means, who governs it, and how that translates to selecting products and services.

HIPAA is comprised of three rules:

- **HIPAA Privacy Rule** – This protects the privacy of individually identifiable health information.
- **HIPAA Security Rule** – This helps set national standards regarding the security of electronic protected health information.
- **HIPAA Breach Notification Rule** – Requires covered entities and business associates to provide notification following a breach of unsecured protected health information.

**As a cloud service provider, we understand navigating HIPAA compliance can be intimidating so we've debunked some common misconceptions for your convenience.**

MISCONCEPTION #1:

## HIPAA compliance can be established solely by partnering with a "compliant" CSP

While many services promote HIPAA compliance, no one product or service makes your company compliant. The Office for Civil Rights enforces these rules, and breach of these statutes can result in severe civil and criminal penalties. (Note* HIPAA compliance certification and "badges" are not given out by any official government agency, a common misconception).

Organizations must understand the rules and implement best practices regarding anyone who comes in contact with protected health information (PHI). They must also deploy products and services that will help accomplish this. A good overall strategy includes implementing administrative, physical, and technical safeguards.

When a company is touting a compliant service, that company is guaranteeing their product has security measures in place that are in line with HIPAA regulations. As these rules are continually changing with evolving technology, individuals should do their due diligence about the features of a service to confirm they are up-to-date with the latest standards.

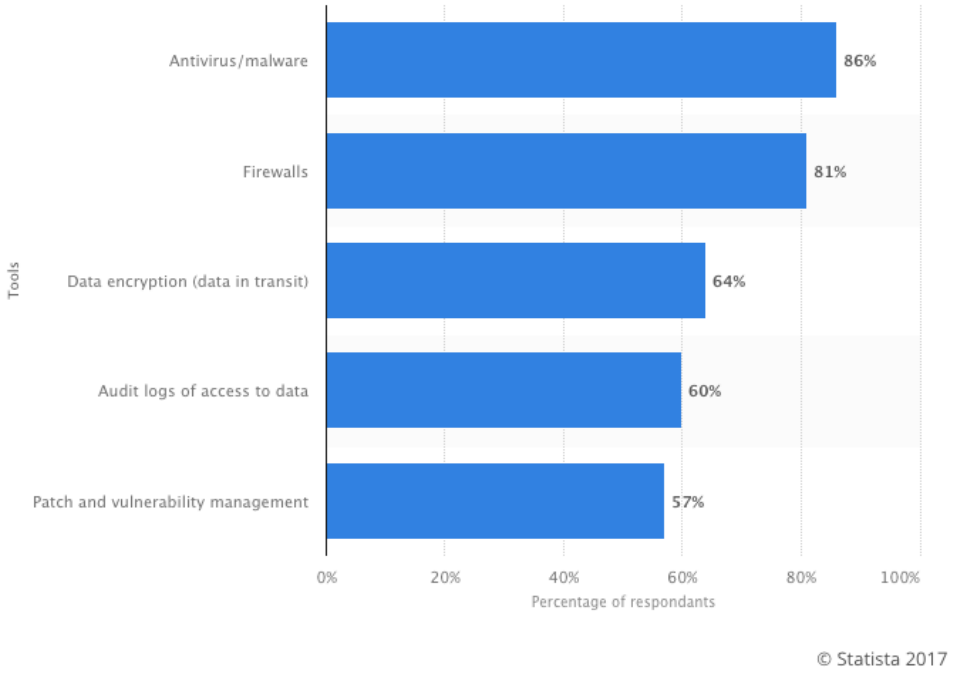
In choosing a cloud service, it might be prudent to ask if the provider is willing to sign a Business Associate Agreement (BAA). A BAA puts in writing the company's accountability to maintain security standards related to the safeguarding of sensitive data.

MISCONCEPTION #2:

## Service providers have the same standards for encryption

It's common when choosing a cloud service provider to rely on encryption to best protect sensitive patient information. With the growing rise of cyber attacks and security concerns, organizations are taking precautions from every angle to safeguard information. These days, encryption alone is not sufficient and should be implemented in tandem with other security protocols.

86% of health companies in the United States use antivirus and malware as the primary tools to secure data, with 64% noting data encryption as a tool commonly utilized. Other IT defenses used to secure health company related data include:




*As the transfer and movement of data increases, encrypting files will become increasingly important. However, not all encryption tools are equal.*

HIPAA guidelines do not define data encryption standards. However, encryption does provide the means through which healthcare providers ensure ePHI have protections. File-level and end-to-end encryptions are used across organizations differently. It's extremely important that a CSP keeps all sensitive data encrypted both at-rest as well as in transit.

MISCONCEPTION #3:

## It is not necessary to assess the CSP you are vetting

Healthcare providers take security seriously and not doing a comprehensive assessment of any cloud service provider could be hazardous to your business. Solutions stated as merely "HIPAA compliant" are not always enough these days. Other security safeguards should be in place to maintain the integrity of your data and the network.

It's imperative to confirm the CSP you are considering checks off the following security protocols:

- Encrypted document exchange
- Secure Socket Layer (SSL) protocol
- User authentication
- Server management security
- Secure application servers, web servers, and networking components
- SSL accelerators configured to maximize uptime
- Data securely backed up regularly
- Perimeter defense with a network protected by firewalls
- Intrusion detection management systems at all times
- Documented DR strategy

This list highlights some of the most critical aspects in addressing security for customers. As technology and infrastructure continue to improve and evolve, it's vital to choose providers that are committed to this evolution as well.

MISCONCEPTION #4:

## Cloud service providers are always to blame for security breaches

Data security, while inconvenient and complicated at times, is a stark reality healthcare professionals must constantly address. Educating employees on how to mitigate risks through administrative, physical, and technical safeguards, is more necessary than ever.

*Gartner predicts 95% of cloud security failures will be the customer's fault by 2020.*

User error is to blame for a significant number of security breaches in organizations. Only a small percentage of the security incidents impacting organizations utilizing cloud services has been a result of vulnerabilities that were the provider's fault. Uninformed or improperly trained users with virtually any system will always have the ability to leverage shoddy practices, which can result in widespread security or compliance breaches (Gartner).

Although diligence should always be a prerequisite before choosing any service provider, secure and reliable cloud solutions are quickly becoming a viable and valuable option for healthcare providers worldwide.

Documo is a next generation document workflow platform. We help businesses move faster by eliminating inefficient document processes.

Securely send, sign, and collaborate on documents from any device.

Please contact us if you're interested in learning more about the product, scheduling a demo, or speaking directly with one of our specialists.

Visit Us: Documo | mFax