mFax

Guide to healthcare fax security

Contents

Startling Healthcare Cybersecurity Stats

Healthcare has become one of the most targeted industries for cybercriminals.

$1.5 M

the maximum fine for a HIPAA violation

$5 T

how much breaches will cost per year by 2024

50x

how much more valuable it is to sell PHI over financial information on the black marketon

41.4 M

patient records have been exposed due to data breaches

572

total number of healthcare data breaches in 2019

More about mFax

mFax is the #1 rated next generation cloud solution for secure, reliable, and feature - rich faxing in the healthcare industry.

Part of the Documo Suite, mFax is built on a highly-reliable, fax-only infrastructure optimized to maximize quality and deliverability.

Why Are We Still Faxing In 2023?

Regulations that govern the healthcare industry including HIPAA and HITECH control how health organizations create, store, interact with, and transmit sensitive patient health information (PHI).

While email works well for fast communication, it does not work in situations requiring the highest security for documents.

Companies in medical, legal, financial, and government-related industries require highly secure ways of sending documents.

Traditionally, these industries relied on fax machines for sending information because the analog nature of faxes doesn't have any openings for hackers to gain access to PHI.

More about mFax

Our highly-rated, fully US-based customer service team stands ready to help you 24•7•365.

Fax Is HIPAA Compliant

HIPAA regulations were created to protect the privacy of patients and to ensure your clientele can trust that you're doing everything you can to make sure breaches of their sensitive information never happen.

While email works well for fast communication, it does not work in situations requiring the highest security for documents.

Companies in medical, legal, financial, and government related industries require highly secure ways of sending documents.

Traditionally, these industries relied on fax machines for sending information because the analog nature of faxes doesn't have any openings for hackers to gain access to PHI.

HIPAA Requirements

The Health Insurance Portability and Accountability Act (HIPAA) is broken up into 3 Rules:

#1 Privacy Rule

This protects the privacy of individually identifiable health information

#2 Security Rule

This helps set national standards regarding the security of electronic protected health information

#3 Breach Notification Rule

Requires covered entities and business associates to provide notification following a breach of unsecured protected health information

When it comes to faxing, whether via analog or digital, the system must follow these guidelines

Correct recipient

Steps must be taken to ensure faxes are sent to the correct recipient and no unnecessary errors are made

Audit trail

There must be a tracking method for where faxes go in case of a data breach or audit

Cover sheet

A cover sheet is required to indicate the confidential nature of the information

Security of Traditional Fax

Sending information via fax might seem simple, but how do you know you aren't breaking the law? Most healthcare companies don't realize physical fax machines store unencrypted fax data that is retrievable by anyone with physical access.

5 Risks of Paper Fax

#1 Misdials

it's easy to misdial a phone number, especially when you're faxing all day long, but this can result in a serious HIPAA violation, even when done unintentionally

#2 Forgotten Faxes

leaving or forgetting to remove sensitive faxes after transmission can expose sensitive information to an unintended recipient

#3 No Audit Trail

No record to prove whether a fax was sent or received or by what user

#4 Forgotten Confidentiality Notices

HIPAA requires all faxes to carry a confidentiality notice

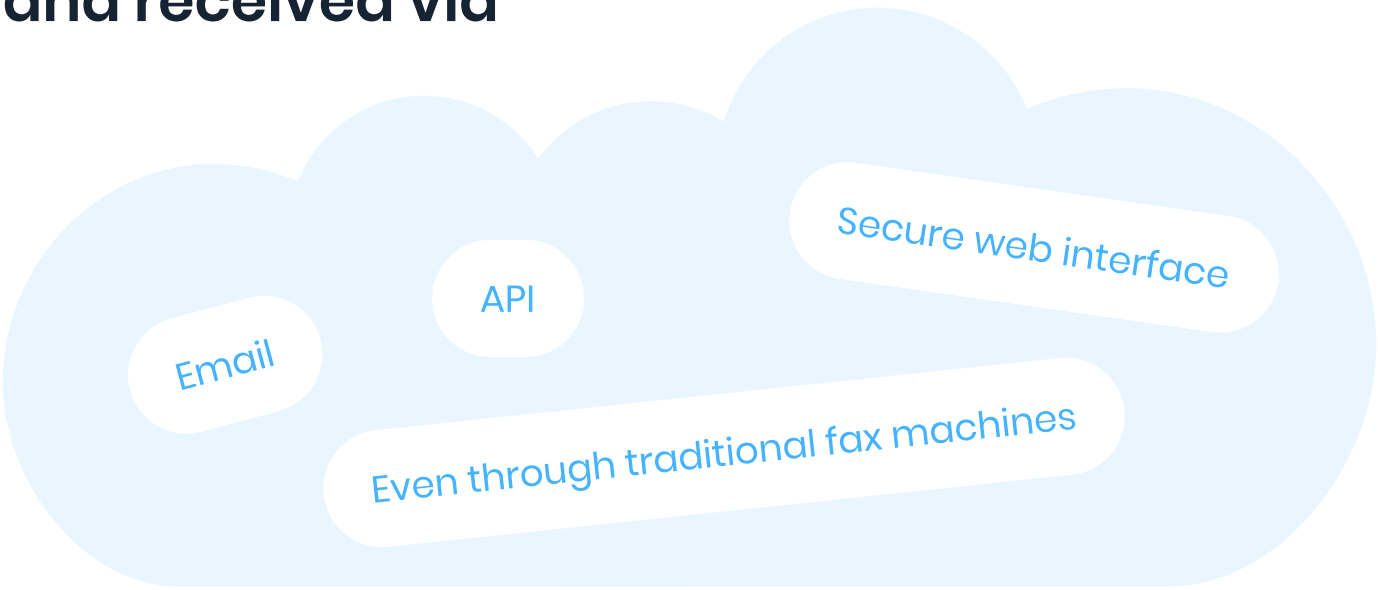
#5 Insecure Phone Lines

Not validating the security of your phone lines leaves each transmission open to being stolen

Cloud Fax

The good news is there are modern options for using fax protocol that don't depend on clunky fax machines or dealing with paper and ink at all.

Cloud fax services allow fax to be sent and received via



Cloud Fax Security

While emails open messages to unauthorized access if a person stays logged into their account and leaves their computer, the same is not true of electronic faxes. Features such as automated log-off keeps idle time on the program from turning into an accidental security breach.

User authentication and administrative controls over who can access what in the system reduces the chances of hackers using a stolen password to get into the server.

With built-in audit trails, you can quickly find out where any fax goes, preventing faxes from missing their destinations.

And encryption during transmission and while on servers protects the information in any faxed documents from unauthorized access.

How Cloud Fax Fills HIPAA Security Holes

Cloud faxing solutions provide quicker workflow and great erreliability than physical fax, and also fills many of the HIPAA security holes created by physical fax:

Cloud fax provides complete audit trails of faxes being sent and received, eliminating the need for physical storage of fax logs

Cloud fax provides individual user accounts and access controls to prevent unauthorized users from viewing faxes

Cloud fax stores fax data in secure servers in the cloud and relies on Tier-1 telecom to transmit the faxes instead of your local phone line

Cloud fax has workflow features that allow you to automatically add cover pages and HIPAA statements to each document being faxed

Cloud fax contains contact records and is easy to error check prior to sending faxes, reducing the odds of sending to an incorrect number

18 Questions to Ask Cloud Fax Providers

Not all cloud fax providers are the same, and it's important that you use due diligence when choosing a HIPAA compliant secure cloud fax solution. Use the following security questions to get you started:

#1 Is all data encrypted both at rest and in transit to prevent unauthorized viewing?

#2 Are web interfaces and API accessible only through secured connections?

#3 Are all document transmissions and log on/log off events recorded along with associated IP addresses?

#4 Do all system access points require user authentication to access secure data?

#5 Does the system include an auto-logoff feature?

#6 Are there advanced administrative controls with customizable user permissions?

#7 Are all web servers, application servers, and database servers housed in state-of-the-art secured facilities with redundant hardware, power, and connectivity?

#8 Do you have a dedicated firewall and intrusion detection systems?

#9 Do your systems have distributed DDoS mitigation plans?

#10 Are systems tested daily for internal security and vulnerabilities?

#11 Is account access able to be limited to only specific IP addresses?

While security concerns are of the utmost importance, don't forget to consider the far - reaching effects of system reliability also.

#12 Do you have documented information security and privacy procedures training for all employees?

#13 Do you regularly perform proactive application and system vulnerability testing?

#14 Will you sign a business associate agreement (BAA) to share in the responsibility of risk management?

#15 Do you rely on a single carrier to route all fax transmissions?

#16 Do you support multiple fax protocols to allow for transmission over all types of networks?

#17 Do you also transmit voice over your fax lines?

#18 What percentage of faxes result in failure? (5-8% is typical, but can be up to 15%)

We know the safety of patient information is the cornerstone of success in healthcare. That's why we've implemented strict security measures and operational features that exceed HIPAA requirements.

At mFax, secure fax isn't just another feature or add-on, it's what we do every single day.

All data is secured both at rest and in transit using powerful 256-bit SSL encryption

Web interface and API only accessible through secure HTTPS connections

Web servers, application servers, and databases housed in state-of-the-art SSAE16 Type II secured facilities

All system access points require authentication to log on. Session auto-timeout. Advanced admin controls with user permissions

Proactive application and system vulnerability testing and daily internal security and vulnerability testing

All transmissions and activity recorded along with associated IP addresses

Google

Built using Google's trusted multi-layer, progressive security cloud infrastructure

Unparalleled Reliability

In healthcare you know there isn't any room for error. We're 100% committed to our record of industry-leading fax reliability. 80% fewer fax failures than other leading cloud providers.

#1 ECM (Error Correction Mode)

Ensures all packets of fax data are received without error

#2 Multiple Carriers

We employ an entire network of premium Tier-1 carriers across North America

#3 Multiple Protocols

We use several fax protocols to ensure delivery

#5 Proprietary Algorithm

Allows us to choose the most efficient and reliable fax routing to ensure information gets to its destination

#5 No Voice

Our lines are 100% dedicated to fax to optimize delivery

Keep your patient data secure by choosing the world's best and most-reliable cloud faxing solution for healthcare.

Get started

Try it for free!

Get in touch with our fax experts

+1 (888) 966-4922

sales@documo.com