mFax

mFax Compliance & Security

Satisfying industry standards & regulations through secure cloud fax

Contents

Insights on how businesses today use fax — 02

How fax use is changing — 02

How secure faxing technology changes the game — 05

Data breaches, ransomware, & cybersecurity in 2020 — 06

Government and Industry regulations on data security — 08

Not all cloud fax providers are the same — 11

mFax compliance & security standards — 11

mFax secure fax technology — 12

The mFax security checklist — 14

More about mFax

mFax is the **#1 rated** next generation enterprise cloud solution for secure and reliable faxing in regulated industries.

Part of the Documo Suite, mFax is built on a carrier grade, fax-only infrastructure optimized for maximum performance.

Our experienced, US-based support team is at your service **24•7•365**.

Insights on how businesses today use fax

International Data Corporation (IDC) surveyed 200 companies in 2017 that had more than 500 employees. They discovered that faxing documents remains a staple in numerous industries. However, changes in recent years have brought this 20th-century technology up to date with modern devices. Businesses can get the security that regulatory agencies require of them by taking advantage of these changes and the newest in fax options with user-friendly interfaces that work in conjunction with their existing workflow software.

How fax use is changing

Faxing has long been a trusted method of communicating in regulated industries such as finance and healthcare, but it has also been used heavily in the government and manufacturing sectors. Nowadays, fax usage has evolved from using a simple phone-line-connected fax machine to integrating network fax machines or cloud faxing into business systems.

For instance, 36% of respondents in the IDC survey reported using standalone fax machines. However, this number dropped to 28% when asked about using this method in the next two years. Companies reporting cloud fax usage jumped from 20% currently using it to 29% expressing a desire to do so in the future. Similarly, fax servers based on a local network remained steady and multifunction printers with fax capabilities dropped from 24% currently using them to 22% choosing this fax method over the next two years. Clearly, cloud faxing is becoming the favored option.

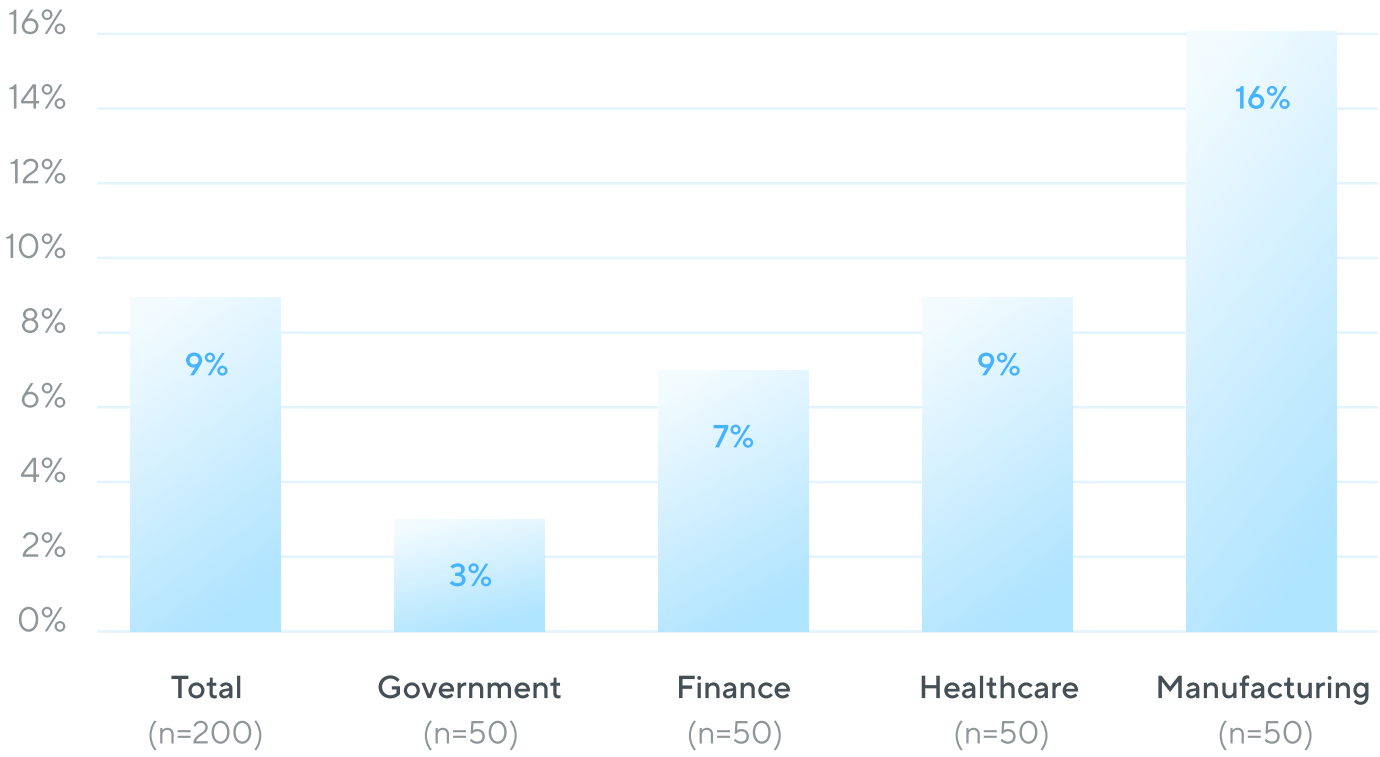
In fact, 90% of companies surveyed by IDC, indicated that they either already integrated electronic or cloud-based faxing into their operations or had plans to do so. This integration allows companies to streamline their workflows and increase productivity.

Despite the fact that faxing has moved past the use of telephone lines and fax machines, these methods will likely not disappear any time soon. Rather, they continue to increase in popularity thanks to technological improvements.

Recent growth in fax usage

Average net Year-to-Year fax usage growth

Q Compared with one year ago, by what percentage did your organization's fax usage increased/decreased/stay the same (net average)?



Source IDC's Fax Survey, February 2017

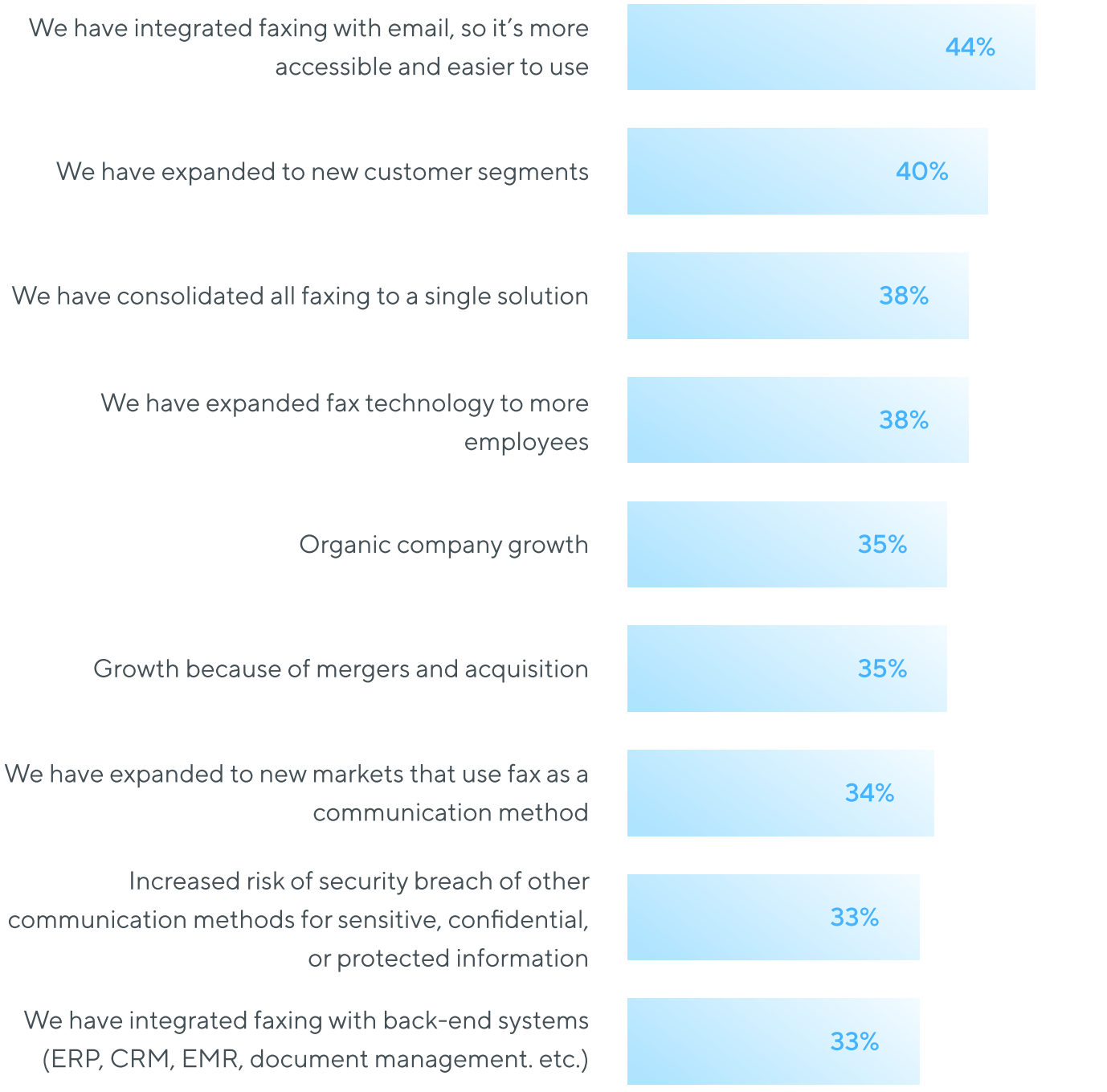
Over the years, fax use for businesses has increased and continues to do so. The IDC survey found 82% of respondents use faxing the same amount or more than a year ago. Additionally, 40% predict their companies will increase its use over the coming two-year period.

Average net year-to-year fax growth for all industries was approximately 9%, with manufacturing reporting a 16% expected growth rate.

Why companies fax more

Top reasons for fax volume growth

Q Whay have fax volumes increased?



Source IDC's Fax Survey, February 2017

This technology is becoming increasingly popular as cloud-based faxing comes with integration technology that facilitates more convenient, secure faxing. Among the companies surveyed, respondents attributed the growth of fax usage to a number of reasons. The largest percentage of companies, 44%, indicated that integrating fax with email made it easier to use and more accessible. Another 33% integrated faxing with their document workflow software, such as EMR, CRM, and ERP. Additionally, 33% of businesses indicated the need for a more secure means of sending sensitive data.

Other drivers for fax use include the many benefits of this technology to companies. Businesses mentioned several advantages of faxing, including a trusted method of data transmission, email integration for easier faxing, quicker delivery of orders and documents, reduced risk of non-compliance, and time-saving efficiencies.

How secure faxing technology changes the game

Faxes have remained very popular because they are not hackable. However, modern technology can render newer fax equipment insecure. Multifunction printers or network-enabled fax machines store unencrypted files on hard drives or send the unprotected files over the local network. Hackers can access these faxes easily, rendering them as insecure as emails.

Changes in the fax industry have not changed the requirements for keeping data secure. Thus, companies must find faxing technology that complies with guidelines for protecting customer and company information. Cloud fax technology must encrypt files going to the server and en route to the server and to the recipient. Whether faxes travel to the server over email, from a fax machine, or from a website, encryption will protect the files and their sensitive data from hackers.

When faxing from a traditional machine, security often means keeping the device in a locked room for employee access only. However, since digital faxing uses a website or email, theoretically, anyone can send or read faxes in the system.

Digital faxing should have user access controls that regulate who can access the server and send or view faxed files. Additionally, audit trails that record who logs into the system and sends or receives faxes will assist with meeting regulations and enhancing security.

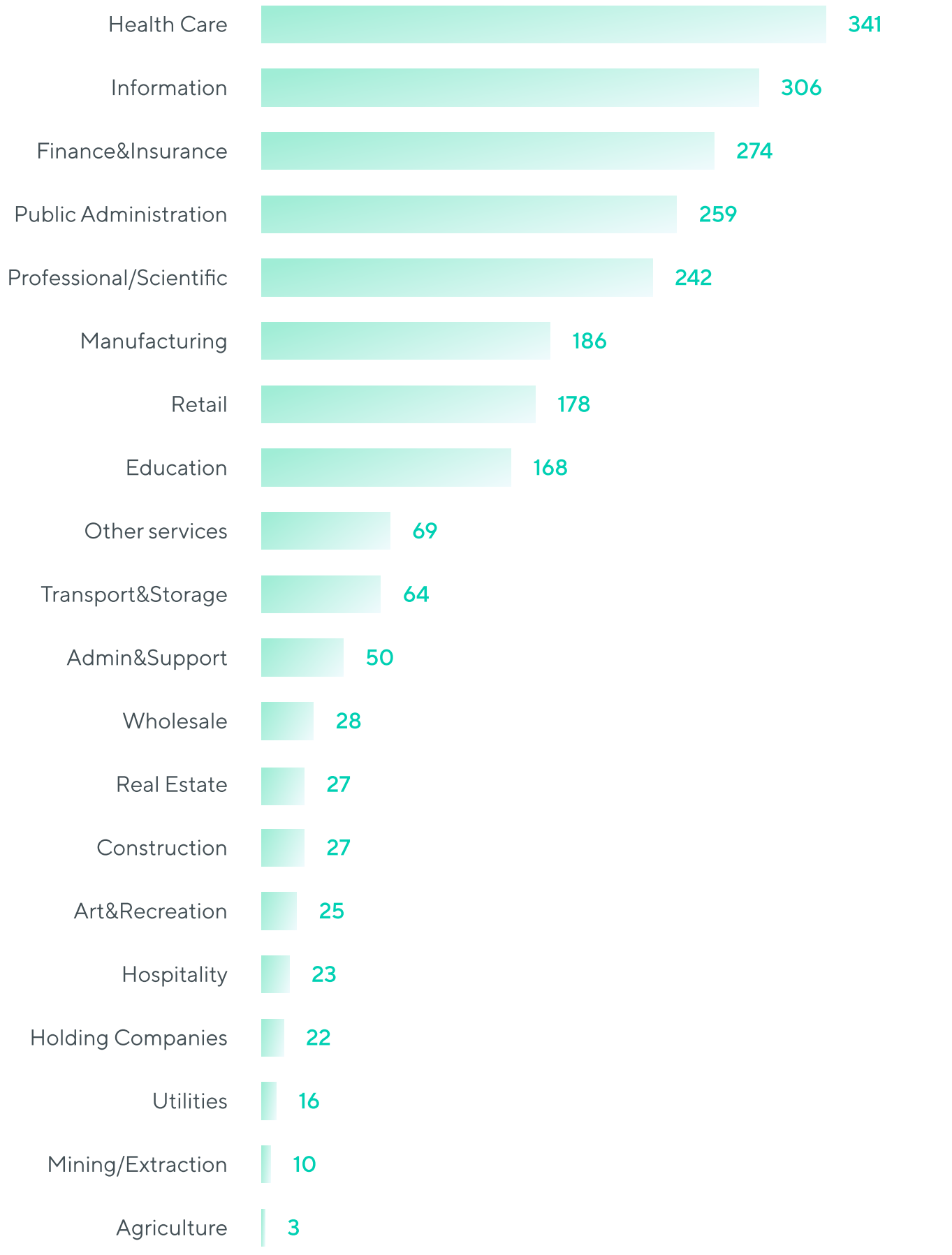
Therefore, a digital fax service meets the regulatory requirements for data protection many companies must adhere to by providing full and complete encryption and other methods of preventing unauthorized access and use.

Data breaches, ransomware, & cybersecurity in 2020

A report by Risk Based Security states that over 36 billion records will have been exposed by malicious actors by Q3 2020, about twice as many records as were exposed in all of 2019.

Malicious actors remain the most common causes of breaches while misconfigured databases and services are the most common cause behind the number of records exposed.

Healthcare remains the most vulnerable economic sector to data breaches in 2020 accounting for 11.5% of reported breaches, with ransomware attacks and employee email hacking being among the most frequent causes.


Health Care
341
Information
306
Finance&Insurance
274
Public Administration
259
Professional/Scientific
242
Manufacturing
186
Retail
178
Education
168
Other services
69
Transport&Storage
64
Admin&Support
50
Wholesale
28
Real Estate
27
Construction
27
Art&Recreation
25
Hospitality
23
Holding Companies
22
Utilities
16
Mining/Extraction
10
Agriculture
3
0
50
100
150
200
250
300
350
400

Government and industry regulations on data security

Several acts and regulations from government entities protect consumer data and privacy. While some regulations are industry-specific, others cover all sectors that handle consumer information. The following acts regulate data transmission, storage, and privacy protection, and apply to all forms of information sharing, including faxing.

Health Information Portability and Accountability Act (HIPAA)

HIPAA requires protecting patient health information from unauthorized viewing through three rules:

- Security breach notification rule
- Privacy rule
- Security rule

The first of these requires healthcare entities to report data security breaches that could expose identifiable patient information. The second guides how facilities protect patient data to prevent others from identifying a patient with their health information. Lastly, the security rule ensures that electronic data storage and transmission protects the information handled to keep it secure.

When it comes to faxing, traditional fax machines only have to take reasonable precautions such as keeping the fax machine in a secure location away from the public and verifying the fax number the data goes to. For online faxing, these measures also apply but in a different way.

For computer-based faxing, unauthorized users cannot see the faxes. Requiring unique and secure passwords for users who log into the system can help meet this requirement.

Additionally, verifying the location where faxes go and the numbers ensure faxes reach their correct destination. However, unlike traditional fax machines, digital faxes can create audit trails that track who logged into the system and where faxes were sent.

Sarbanes-Oxley (SOX) Act

SOX compliance applies to all industries because this act governs the handling of electronic and physical records of accounting data. Accounting departments must undergo audits by a SOX-compliance expert to help the company find and fix security gaps. After fixing the holes, companies must meet the following to maintain and continue compliance with SOX:

- Prevent data tampering with their accounting information
- Use software or systems that create timestamps of all information that comes into the system to later create a timeline of incoming data
- Have a method to track and monitor access to data
- Verify and report on security and safeguard effectiveness
- Immediately identify security breaches
- Report to SOX auditors safeguards, failures of safeguards, and security breaches

When it comes to faxing, tracking how users access the system and when faxes are sent and received via an audit trail can help ensure SOX compliance.

Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley (GLBA) Act covers financial institutions that have significant engagement in financial activities. Under the GLBA Privacy Act, these institutions must share their company's privacy practices with their customers,

which includes information collected from customers, how the business uses that data, and if they share the information with third parties.

In addition to a privacy notice, institutions must also allow customers to opt out in a reasonably easy way from having their nonpublic information shared with third parties.

Additionally, GLBA has a Safeguards Rule that requires financial institutions to create a method for protecting customer information. Outlined in the method should be how the institution gathers, uses, access, distributes, protects, transmits, and otherwise handles customer information. In making a plan for protecting customer information, the institution must determine if they have gaps in their data security and find ways to close those.

When it comes to faxing within compliance of GLBA, financial institutions must ensure that only those authorized access to the faxed information can see it and that a third party cannot intercept the data in transit.

Payment Card Industry Data Security Standard (PCI DSS)

Unlike other regulations, the PCI DSS is not from a government body but an independent group created by a gathering of the major credit lending companies – Visa, JCB, Discover, American Express, and MasterCard – known as the Payment Card Industry Security Standards (PCI SSC). All industries that handle credit cardholder information must adhere to the PCI DSS guidelines.

Electronic and paper handling of credit cardholder information must be secure and protected from security breaches. The PCI DSS compliance process involves three steps, the first of which is having an assessment by a data security firm qualified to make an evaluation of the business's system. Next, the company must fix any issues discovered during the assessment. Lastly, businesses may need to submit regular reports to the credit card companies and financial institutions on their PCI DSS compliance.

When credit cardholder information is being sent and received using cloud fax, it must be protected from data breaches while in storage and transit. In addition, only those allowed access to the information should have the ability to view faxes that contain this information.

Not all cloud fax providers are the same

Cloud fax providers differ widely in their ability to deliver a solution that helps your organization achieve and maintain compliance with a wide range of regulatory measures and privacy laws intended to protect sensitive data. Many online fax providers do not offer the required privacy, security, and administrative tools necessary for compliance with some of the more stringent regulations, like HIPAA, GLBA, SOX, and PCI. While many providers may claim to be compliant with any given set of regulations, they are often unwilling to sign a business associate agreement (BAA) as required by HIPAA, which should raise greater concerns about their actual commitment to privacy, security, and compliance issues.

mFax compliance


mFax is designed for secure and compliant faxing that meets or exceeds even the toughest standards set by HIPAA, GLBA, SOX, and PCI.

mFax leverages the Google Security Model, using the same secure-by-design infrastructure, built-in protections, and global network used by Google to protect information, identities, applications, and devices.

Business associate agreements are available to all customers to ensure HIPAA compliance, and as proof of mFax's commitment to the highest security standards for all applications and products.

mFax security measures

mFax is an enterprise-grade, cloud-based online fax solution used by companies in highly regulated industries to securely send and receive sensitive information. As a result, the platform supports AES 256-bit encryption for all documents at rest and Transport Layer Security (TLS) version 1.2 for data in transit, as recommended by the National Institute for Standards and Technology.

In compliance with Payment Card Industry's Data Security Standard (PCI-DSS), TLS 1.2 ensures the safeguarding of all sensitive payment information and cardholder data contained in transmissions.

In accordance with industry standards and federal guidelines, mFax protects personally identifiable information (PII) and other sensitive information while in storage (at rest). NIST recommends a minimum Advanced Encryption Standard (AES) key strength of 128-bits. mFax uses 256-bit encryption keys to increase the protection of all stored data.

Some manufacturers continue to use outdated encryption standards such as DES (3DES), which are protocols that were first used in the 1990s. Once NIST deprecates that algorithm, those fax servers will no longer be compliant for the storage of ePHI and other sensitive data.

mFax secure fax technology

mFax comes standard with the highest levels of security, including AES 256-bit data encryption for all information at rest, and uses TLS 1.2 encryption for data being transmitted.

Optional email notifications of incoming faxes include a link to a secure connection (HTTPS) URL where a user must login with their userID and secure password (or access a secure read-only portal) to view or download faxes.

mFax secure API

mFax's developer-friendly API can be integrated into a variety of existing workflow systems to add high-volume fax capabilities where users need it most.

All information processed through the mFax API is secured using AES-256 bit encryption for at-rest information in storage and TLS 1.2 encryption for information being transmitted.

mFax hierarchical administration portal

mFax includes a robust and feature-packed admin portal so that administrators can easily add, delete, and manage users. It also lets admins track fax volumes, see fax sending data, and restrict access based on IP address.

To enhance security, the user settings are highly flexible, with the ability for admins to set multiple access levels with granular permissions to protect your most sensitive data.

mFax's hierarchical administration features give administrators complete control over data access, enabling them to create groups and subgroups across multiple locations or departments.

The mFax security checklist

- HIPAA compliant & secure
- We sign business associate agreements (BAAs)
- PCI-DSS, GLBA, SOX compliant
- Data at rest (in storage) protected by AES 256-bit encryption
- Leverages Google Security Model for cloud based infrastructure
- Web interface and API only accessible through secure HTTPS connection
- Web servers, application servers, and databases housed in SSAE16 Type II secured facilities
- All system access points require authentication to logon
- All transmissions and activity are recorded along with associated IP addresses for easy auditing
- 24/7/365 knowledgeable, US-based customer support

mFax

Ready to Get Started?

Contact us at sales@documo.com or call us at (888) 966-4922