eFaxCorporate®

SECURE CLOUD FAXING FOR HIGHLY REGULATED INDUSTRIES:
A Practical Guide to Cloud Service Migration for Finance, Legal, Health and Education

Table of Contents

Introduction

In a humorous exchange on the NBC comedy series The Office, David Wallace, chief financial officer of the show's fictional company Dunder Mifflin, says to regional manager Michael Scott, "I'll fax over some of the things we're looking for, okay?" Scott responds, "Fax? Why don't you just send it over on a dinosaur?"

Given our ability in the twenty-first century to store, access and transmit all of our data electronically — without the need to print paper hardcopies — Scott's reaction is understandable.

> *"Fax? Why don't you just send it over on a dinosaur?"*

In our modern era of email and unified cloud collaboration services, where document sharing is instantaneous and entirely virtual, it can be difficult for a professional in an industry that no longer relies on fax to understand the need for an analog technology that uses paper and audio tones to transmit documents across the public telephone network.

But if you are in one of the many industries that still relies on faxing for your company's typical communications — particularly highly regulated industries such as healthcare, legal or financial services — you know that faxing as a communication protocol is here to stay for the foreseeable future.

Moreover, as you migrate other communications and technologies to more streamlined protocols, the existing fax environment of desktop fax machines, dedicated fax lines and fax servers is probably becoming an increasingly troublesome and costly infrastructure to manage.

There are many reasons businesses in these industries continue to fax — from the fact that many of their partners and customers demand it, to the fact that these businesses feel confident that faxing can keep them on the right side of data-privacy regulations, to the understandable desire to maximize the return on their large investment in legacy fax infrastructure.

But as this paper will show, businesses in particular vertical industries that still need to use fax as part of their daily communications do not need to choose between maintaining their legacy fax infrastructure or finding a different communication protocol.

There is a solution that will allow them to continue to support robust business-faxing capability while at the same time leveraging all of the cost-savings, security and productivity benefits of modern-day Internet technologies.

That solution is cloud faxing.

This paper will also walk you through some of the common pitfalls in migrating fax or any new technology to a cloud environment, and it will then provide you with a helpful checklist of key traits to look for when selecting your cloud fax vendor.

After reading this paper, we are confident that you will find cloud faxing the ideal way to seamlessly move your company's legacy fax environment to a more convenient, cost-effective, secure and compliant methodology — without sacrificing any of the fax functionality your employees need to perform their jobs effectively.

Why Fax is Still in Widespread Use in Industries Such as Healthcare, Finance and Legal

When you consider that one of the trends in the healthcare industry today patients wear Internet-of-Things (IoT)-enabled devices such as watches and bracelets, which take real-time readings of their health data and send that data to their doctors over the web, it can be difficult to understand why such an industry would still communicate by feeding paper through a desktop fax machine for transmission over plain old telephone lines.
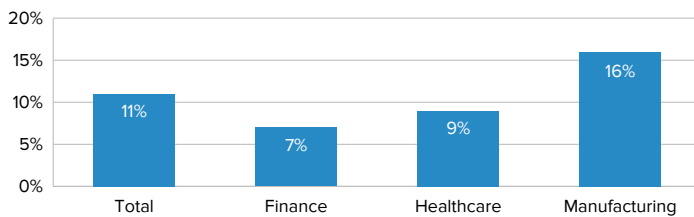
2017 Net Fax Usage Growth - Year over Year 2015-16
Source: IDC's Fax Survey 2017

Or consider the 'fintech' innovations coming from the banking and financial services industry. Most of today's banks offer free apps that allow customers to transmit money from their accounts via text message, and deposit a check from anywhere by simply photographing it using their smartphone's camera. And yet this industry, too, still relies on the 1980s technology to transmit many of its most important and time-sensitive documents. And that usage is still growing, as shown in the chart above.

Mortgage applications, for example, require 'wet' signatures that may need to be notarized and typically must be sent to the bank by postal mail or expensive courier services--or they can be faxed.

What's going on here? Why would such industries, which are pioneering technological innovations, still use outdated protocols for communication — particularly when much more advanced services like email are readily available?

First, let's discuss some of the types of communications these industries still prefer (or are required by regulators) to send and receive by fax. Then we'll discuss the reasoning behind these industries' continued loyalty to this aged technology.

Law Firms Still Use Fax for:
- Contracts
- Client invoices
- Courthouse documents
- Communications with other law firms

Why is the legal industry among the most prolific faxing industries today?

Perhaps it is because so many law firms have already invested in expensive in-house fax infrastructure, consisting of multi-line fax machines and multi-function printers with fax capabilities, fax server hardware and software, and the necessary communications lines.

Or perhaps it is simple inertia leads these firms to continue with their legacy faxing processes — because they always have. Many senior lawyers and their assistants have been doing things this way for decades and have no real incentive to change.

From one-person legal operations to large firms, lawyers and their administrative staff in 2017 still often use fax for client billing, communicating with court clerks — asking them for docket sheets or copies of pleadings, — and a host of other reasons.

The legal system itself can perpetuate the use of fax as a commonly accepted means of communications. For example, a precedent-setting court decision described fax as "a reasonable and increasingly common means of modern communication" [California Court of Appeals in Hofer v. Young, 38 Cal. App. 4th 52 (1995)].

Furthermore, fax (but not email) is listed as a Proof of Service delivery option in civil filings for California courts in 2017, as shown below.

ATTORNEY OR PARTY WITHOUT ATTORNEY:	STATE BAR NO:		FOR COURT USE ONLY
NAME:			
FIRM NAME:			
STREET ADDRESS:			
CITY:	STATE:	ZIP CODE:	
TELEPHONE NO:	FAX NO:		
E-MAIL ADDRESS:			
ATTORNEY FOR *(NAME)*:			

SUPERIOR COURT OF CALIFORNIA, COUNTY OF
  STREET ADDRESS:
  MAILING ADDRESS:
CITY AND ZIP CODE:
    BRANCH NAME:

	CASE NUMBER:
Plaintiff/Petitioner:	
Defendant/Respondent:	CASE NUMBER:

PROOF OR SERVICE—CIVIL

Check method of service *(only one)*:
☐ By Personal Service   ☐ By Mail   ☐ By Overnight Delivery   CASE NUMBER:
☐ By Messenger Service   ☐ By Fax

Do not use this form to show service of a summons and complaint or for electronic service.

See USE OF THIS FORM on page 3.

1. At the time of the service I was over 18 years of age and not a party to this action.
2. My residence or business address is:

3. ☐   The fax numberfrom which I served the documents is *(complete if service was by fax)*:

In addition, electronic copies of contracts, such as photocopied, faxed and scanned or electronically stored versions, are all considered enforceable contracts.

And even if they wanted to retire their costly and clunky onsite fax hardware, law firms really can't get rid of fax entirely. That's because many of the third parties a firm deals with on a regular basis — from clients, to insurance companies, to courthouse staff, to other law firms—will continue to prefer or even demand to communicate via fax.

For example, marking up legal contracts is a common practice, and often the more senior partners in a law firm will prefer to print out and read the contract, marking it up by hand.

They (or an assistant) could then scan the document, walk back to their desk, find the email containing the scan, rename the scanned file, open and address an email, attach the image file to an unencrypted email message and transmit it to the opposite party— or they can simply place it on the fax machine or multifunction printer, enter the fax number and hit send, secure in the knowledge that a fax is not likely to be intercepted during transmission over the public telephone network,

and that they will have a delivery confirmation when the transmission is complete.

In fact, because of this end-to-end transmission record, which is generated by a message from the recipient's fax machine, fax is an acceptable means of serving and filing legal papers in many jurisdictions.

Email, on the other hand, is not, because there is no reliable means of confirming delivery, which would allow the opposing party to claim they never received the document.

Good lawyers are also highly security conscious, and most will not knowingly send confidential customer information, financial information, account numbers, passwords, etc. by unsecured email, especially when there are risks to discovery in ongoing litigation and the possibility of jeopardizing client privilege.

The only other secure alternative is by courier or overnight delivery services which are slow and expensive compared with fax. And if the documents are time sensitive, fax is clearly the preferred means of communication to physical delivery services.

Another likely reason for the persistence of fax is that many of the key documents law firms send and receive by fax require 'wet ink' signatures.

While acceptance of Digital Signatures is codified in law by the E-Sign act [Electronic Signatures In Global And National Commerce Act], a number of exceptions were made for the following:

- Official court documents (including briefs and pleadings)
- Court orders and notices
- Divorce decrees
- Adoption paperwork
- Wills, codicils, and trusts
- Notices of termination of utility services
- Notices of default, foreclosure, repossession, or eviction

- Cancellation of insurance benefits
- Product recalls or notice of material failures
- Documentation accompanying the transportation of hazardous materials
- Parts of the Uniform Commercial Code

Moreover, because the signatures on faxes are accepted as legally valid in most states, this is often seen as the simpler and safer method and more likely to keep legal entities compliant with regulators.

Whatever the reason, the legal profession still relies heavily on fax for their day-to-day communications.

Healthcare Companies Still Use Fax for:
- Insurance claims, denials, appeals
- Billing and medical record requests
- Prescriptions and refills for pharmacies
- Lab requisitions
- Clinical Field Trial Results

The story is much the same in healthcare. And in the health profession the persistence of an analog technology like fax is even more peculiar — considering that this industry is inventing some of the most advanced technology in the world to treat disease and prolong life.

But fax still plays a vital role in most healthcare organizations' daily communications, from the smallest single physician practices to the largest hospital chains, including their most important applications such as patient clinical data, prescriptions, insurance claims and invoices.

As the medical publication *Healthcare Insighter* points out, the healthcare industry still favors fax so much that it continues to enforce some completely counterintuitive rules.

Here are a couple of the more bizarre examples…

Generating a lab requisition requires that a rubber-stamp signature be authenticated by initials and the date written in ink pen. But… if that same lab requisition is faxed, there is no authentication requirement at all.

If a pharmacy receives a hardcopy prescription with a digital image of the doctor's signature, they often require that the doctor re-sign that prescription in ink beside the digital image. But… if the doctor's office instead faxes that prescription, the pharmacy will accept the digital image of the signature alone.

> *…if that same lab requisition is faxed, there is no authentication requirement"*

Meanwhile health insurers require that claims and expense reimbursements be faxed to them, and the level of faxes sent and received at companies that manage claims processing can easily reach many tens of thousands of pages per month, or more.

What all of this points to is that today, and for the foreseeable future, fax will continue to be a necessary part of many healthcare communication systems.

And finally, there is a widespread perception that traditional analog fax, by virtue of the fact that it runs over the telephone network and not the Internet, is inherently secure.

And thanks to the Conduit Exception Rule, this type of communication is generally exempt from the encryption requirements of HIPAA, the Healthcare Insurance Portability and Accountability Act, that was designed to protect the privacy and security of healthcare customers.

This perception is not always true, as shown below, but such perceptions can be very hard to break when they are thoroughly entrenched in an industry.

In fact, there are potential HIPAA compliance pitfalls with traditional fax machines.

For example:

- Fat-fingering fax numbers is a common source of complaints to the Dept. of Health & Human Services Office of Civil Rights (HSS-OCR) which is responsible for HIPAA compliance.
- If you fax PHI to an unauthorized recipient, you have just committed a HIPAA violation. It doesn't matter if it was done by mistake.
- Documents containing PHI left unattended on the machines are vulnerable to unauthorized viewers.
- If you don't have a written policy that specifies a set of procedures to secure faxed PHI at both ends, you are not in compliance.

And now consider that Cloud-based fax-by-email, which goes from desktop to desktop, when fully encrypted during transmission, is inherently more secure and complaint than traditional analog fax. We'll explain in more detail about how that works later.

Financial-Services Firms Still Use Fax for:
- Loan documents
- Mortgage applications
- Stock-transfer & trade confirmations
- Tax forms

Businesses in the financial services industry also continue to use fax for many important communications, and in this industry's case it is often out of an abundance of concern for security and regulatory compliance.

For example, many banks still require mortgage and other loan applications, as well as other type of financial documents, to be delivered in person, by U.S. Mail or delivery services like FedEx or UPS, or by Fax.

So fax is the only electronic delivery service that is acceptable to many banks and finance companies for multiple types of legal documents.

Financing Bank

You can *FAX* your application
123-456-7890

Home Equity Loan Application

IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT
To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

What type of account are you applying for? (Please check appropriate box):
☐ INDIVIDUAL (Own income or assets)
☐ JOINT (both borrowers please initial that you applying jointly) _____ _____

Loan Product
☐ Home Equity Loan for a fixed term of ☐ 5 years ☐ 10 years ☐ 15 years ☐ 20 years ☐ Home Equity Flexible Line of Credit

Amount requested	Purpose of loan	Referred By (Bank Use Only)

Borrower Information

Full Name	Social Security Number	Date of Birth	Marital Status: ☐ Married ☐ Separated ☐ Unmarried - (Single, Divorced, Widowed)	Residency Status: ☐ U.S. Citizen ☐ Permanent Resident Alien ☐ Non-Perm Resident Alien ☐ Other
Principal Residence Street Address, City, State, Zip		Home Phone		
Current Employer	Position or Title	Work Phone		
Employer's Address			☐ Full Time ☐ Part Time	Years There	Occupation (Prior if Retired)
Gross Salary ☐ Week ☐ Month ☐ Year	Other Income* ☐ Week ☐ Month ☐ Year	Source of Other Income*		
Previous Employer	Position or Title	Work Phone	Years There	Occupation
Previous Employer (2)	Position or Title	Work Phone	Years There	Occupation
Driver's License Number and State	Issue Date	Exp Date	Cell Phone	E-mail Address
Name of Nearest Relative	Relationship	Phone Number	Mother's Maiden Name

Alimony, Child Support, or Separate Maintenance Income need not be revealed if you do not wish to have it considered as a basis for repaying this obligation).

General compliance with industry regulatory regimes such as Sarbanes Oxley requires that financial services firms track all electronic messaging and paper-based transactions, including the ability to log, store and retrieve them securely while maintaining client confidentiality.

Academic Institutions Still Use Fax for:
- Student transcripts
- Applications
- Financial aid forms
- Ordering supplies

Many K-12 school districts continue to use standalone fax machines and multifunction printers for faxing between school offices because a. it's there, b. it's convenient since everyone knows how to use it, and c. it's considered a secure means of communications with other organizations, especially in municipal government, with whom they need to communicate.

With tight or declining IT budgets, there is little incentive to migrate to a new system that would require additional capital budget requests and the operational expense of staff retraining.

For higher educational institutions such as colleges and universities, faxing also remains a common form of communication. In the case of this industry, however, all evidence suggests this is primarily due to inertia — it's simply always been a standard way for schools to send and receive student documentation and application paperwork.

Plus, state and federal regulations regarding privacy of student records create additional incentives to stick with fax that is considered a secure means of communication with parents or state agencies.

Similar to the other regulated industries we've been discussing to this point, academic institutions have invested heavily in in-house fax infrastructure and they continue to derive some value from that infrastructure. There might also be the sunk-cost fallacy at work here — these institutions are willing to put up with increasingly cumbersome onsite fax hardware to amortize their original investments in purchasing and deploying this infrastructure.

But universities are beginning to discourage fax as the default means of communication with students, parents, vendors and other third parties. For example, The Financial Aid page on Cornell University's website is just one instance of colleges now tending to favor other forms of communication over fax.

Why Do These Industries Continue to Use Fax?

For two decades, eFax Corporate® has worked with thousands of organizations of all sizes, in virtually all industries. Partnering with such a wide variety of businesses, providing cloud-fax capability for their mission-critical faxes over such an extended period of time, has given us a unique understanding of the goals, needs and concerns these enterprises have for their fax processes.

Here are three primary reasons we have identified for why regulated organizations — in healthcare, financial services, the law, education,

manufacturing, government, etc. — are sticking with fax.

Money: The sunk-cost fallacy

One key reason businesses are slow to migrate away from analog fax is that they've already invested in setting up their company-wide fax environment — expensive fax server hardware and software, desktop fax machines or multifunction printers, dedicated fax lines, and all of the related services such as fax-gateway licenses and perhaps server racks at a colo. Organizations understandably want to continue using these systems as long as possible, to reap the most ROI from those investments, especially if the expense has not yet been fully depreciated.

While using sunk costs as a reason to continue a particular process is not always rational, in the real-world many businesses will make decisions on the basis of not wanting the past investment to be seen as wasted, even though the product or service may have outlived its usefulness.

Security: Fax is Still More Secure than Email

With all of the recent high-profile stories of businesses, politicians and even highly secretive government agencies like the National Security Agency (NSA) suffering computer-system and email data breaches, it is understandable that regulated businesses have concerns about migrating all of their fax communications to email, especially in industries that are subject to regulatory oversight with financial penalties for non-compliance.

Many of these businesses are targets of cyber hacking — particularly healthcare and financial firms — because they handle such personal information on their patients and clients. Such businesses are also heavily regulated by federal laws and regulatory rules, such as HIPAA for healthcare and Gramm-Leach-Bliley Act (GLBA) for finance.

Document security and customer/patient confidentiality is therefore a top priority at these organizations. Moreover, fax is generally perceived as more secure than email, and its use is even given formal recognition in the federal register.

An analog fax transmission going across the public telephone network can be more difficult, if not impossible, to intercept from a remote location than an email transmitted over the Internet, unless that email message is secured with strong encryption and authentication.

Compliance: Government Regulators Often Prefer Fax

This is the often the primary reason so many businesses in regulated industries are reluctant to upgrade their fax infrastructure in any way.

Even though their legacy fax systems might be expensive, time-consuming for IT to maintain, and prone to technical problems, these businesses know the regulatory bodies that enforce data privacy rules in their industries often prefer faxing to more modern communications.

With that in mind, here is a brief overview of how federal regulations affect the fax processes of regulated businesses. We will then offer an alternative process, cloud fax, which satisfies both the need for continued fax capability and the advantages of migrating to the cloud — all while actually improving your compliance position.

How Regulation Affects' Companies' Fax Processes

Because so many businesses today handle personally identifiable information — or "PII" — of their customers, more organizations fall under the complex regulatory infrastructure of the numerous and overlapping federal/state laws and agencies governing data privacy.

Healthcare Regulations

The Healthcare Insurance and Portability Act (HIPAA) regulates healthcare organizations — called 'Covered Entities' — as well as any 'Business Associates' of these entities, that handle patients' records in electronic format.

The HIPAA final regulations specifically exempted fax (and telephone) from inclusion as an electronic communications medium (Sec. 160.103 - Definitions). Fax transmissions (and telephone calls) are therefore not covered by HIPAA.

However, any document containing 'protected healthcare information,' or PHI, sitting on a fax machine's input or output tray, or in its internal storage, would be subject to the HIPAA privacy rules, and more than a few companies have received fines or 'corrective action' for forgetting to secure the fax machine itself.

Nevertheless, the exemption of fax from the definition of electronic communication under HIPAA has created the widespread perception that fax is immune from HIPAA. This perception, which is only half true, has contributed to the persistence of fax as a common method of communication throughout the healthcare industry.

Similarly, when eFax Corporate® transmits faxes via email, which would normally be covered by HIPAA, that transmission is exempted by what is known as the 'Conduit Exception.' This exemption treats the providers of Cloud-based fax services the same the post office or telephone company, since they are providing 'mere data transportation service' on behalf of a covered healthcare company.

The Conduit Exception is based on the fact that any processing is incidental to the transmission process, and any storage of the fax during that processing is temporary.

However, when faxes are stored on a "more than temporary basis," such as if the cloud fax service archives customer faxes for later retrieval, that service would be covered by HIPAA and those stored faxes would need to be protected according to HIPAA privacy and security requirements. The company providing that covered service would also be considered a Business Associate of the healthcare provider that is sending the faxes, and would need to sign a Business Associate Agreement with its healthcare client.

Financial Industry Regulations
Financial services businesses are regulated by the federal Gramm-Leach-Bliley Act (GLBA), which sets strict demands for safeguarding personal customer information.

Interestingly, the law defines a 'financial services' business quite broadly, to include any company that offers any lending or credit service to its customers. This means companies that might never think of themselves as part of the financial-services industries — such as retailers that offer their own credit cards or even real estate brokerage firms — are indeed considered financial businesses and subject to GBLA.

Then there is Sarbanes-Oxley, or 'SOX,' which governs data privacy for any publically traded company. In addition, many states have passed their own data privacy regulations, some of which are even stricter than the federal regulations. These laws are enforced by the State Attorney Generals for the respective states.

Education Privacy Regulations
Educational institutions — primarily colleges and universities — are regulated by the federal data privacy law FERPA, which demands strict protection of the financial, academic and other personal information on students and their families. And organizations that provide health care for students are also subject to HIPAA.

The list goes on….

There are also a number of non-governmental regulatory bodies developed by the industries themselves to police their members.

For example, FINRA, an independent (non-governmental) regulator, acts as a data privacy watchdog over financial securities dealers and exchanges. The legal profession has its Model Rules of Conduct, overseen by the American Bar Association. And the credit card industry has its Payment Card Industry Security Standards Council which issues and updates the Payment Card Industry-Data Security Standard (PCI-DSS), with which all companies who process credit card payments must comply.

GLBA   HIPAA   Sarbanes Oxley
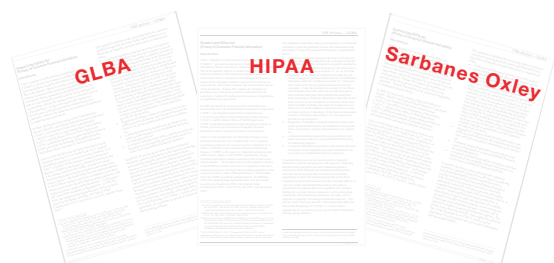
What's important to understand about these laws and independent regulatory codes is that they are almost all written in dense legalese — and some run hundreds of pages. Moreover, they're written intentionally vaguely, not prescribing specific measures that a business is expected to take to ensure its customers' data privacy.

The regulators explain that they crafted the laws this way to allow for inevitable new processes and technologies that would emerge after the laws were written. This makes sense. But it also makes it difficult for any regulated business — even those with the most sophisticated IT teams — to know if they are truly in full compliance with their industry's data privacy laws. Which is why so many regulated businesses have been reluctant to move away from the regulatory comfort of transmitting their customers' personal information by fax — even if it is far more cumbersome a method than others.

What is Cloud Faxing — and Why is it Superior to Traditional Fax Technologies?

In its most common form, electronic or 'cloud' based faxing is a very simple concept whereby your staff can use their standard email programs to send and receive faxes. Cloud fax can also mean faxing through a secure web portal, or faxing directly from employees' mobile devices using a mobile fax app. The main point of this approach is that you no longer need to be tied to physical machines attached to analog phone lines in order to send or receive faxes.

With the right cloud fax partner, you can even send and receive faxes using applications integrated into your business's existing workflow applications such as SAP or Salesforce, or faxing by email through your multifunction printers — which can be helpful when you want to scan and fax a hardcopy document by email in one step, such as those requiring a 'wet ink' signature.

How Cloud Faxing Works

As you can see from the diagram here, with a cloud fax service you'll have your faxes transmitted over the Internet as simple email attachments. In other words, your fax messages start their journey as natively digital, not as analog fax images that need to transcoded into digital formats multiple times along the way.

1. Open an email message
2. Attach your fax docs and send
3. Your recipient receives a standard fax

And the process works exactly the same in reverse; inbound analog faxes sent from fax machines are converted to digital documents, either PDF or TIFF (image) formats, and arrive in your inbox attached to an email message.

Your cloud fax provider will assign your company real fax numbers — as many as you want. Which means that when you send or receive a fax, you'll be using a real business fax number, with your choice of local or toll-free area code, and the other party won't know the difference.

With a good cloud fax provider, you will be able to move, or "port" your existing fax numbers over to the new service so there is no need to publish new fax numbers.

As with most cloud-based services, you won't need a buy, install or maintain fax machines, fax servers or any other traditional on-premises hardware/software system to receive or send a fax. And you can disconnect those analog or digital telecom lines since all faxes will run over your Internet connection.

Okay, now that we have a good high-level understanding of how cloud faxing can work, let me get back to the money, security and compliance benefits of cloud-based faxing.

What are the Benefits of Cloud Fax?

You'll Save Money

Depending on the size of your organization and volume of faxing, upgrading to the cloud can eliminate a significant upfront capital and operational expense including the monthly recurring telco line charges, not to mention the IT overhead to keep it all running. Fax machines, for example, need continuous replacement of paper and toner, which can add up over the course of a year, and a maintenance contract because they malfunction easily.

For higher volume faxing, as in the insurance and healthcare industries, most companies began installing fax servers as far back as the 1980s. Here is a rough approximation of fax server lifecycle costs for small and large offices:

Fax Server Hardware:	$2,000 and up
Fax Card:	
Dual analog ports	$1,500
T-1 PRI 24 channel	$17,000
Fax Server Software:	
Small business license - single channel	$3,300 (+$749 per add. channel)
Enterprise Suite/server license - single channel	$17,000 (+$749 per add. channel)
Total Capital Cost:	
Small Office	$ 7,549
Large Office	$53,227
3 year amortization:	
Small Office – 2 lines	$2,516 per year
Large Office – 24 Lines	$17,742 per yr.
Recurring Charges:	
Single analog line	$60/month
T-1 PRI	$400/month
Software Maintenance:	20-25% of software cost per year.
Total Annual Cost	
Small Office	$4,459 per year
Large Office	$23,778 per year
Note: Costs shown are based on discounted prices from leading hardware and software vendors. Your costs will vary by vendor, network size and configuration.	

Clearly, maintaining a legacy fax environment is expensive. In addition to the basic costs of Fax Server software packages, every added feature costs extra. Want to connect multifunction printers? Add $500 for an MFP license, per printer. Want to archive your faxes? That's another software module for extra $$$ plus additional storage drives that increase the overall cost.

There are also several additional 'hidden' costs — many of which most businesses never factor into their estimates of what they're really paying to maintain fax operations in-house. These include electricity needed to power all of your fax servers and machines, possible rack space in a colocation facility, as well as the ongoing costs of IT management, maintenance and troubleshooting. (Fax servers are notorious for crashing, requiring IT personnel to reboot the down server and assess the level of damage.)

And you will likely also need to dedicate internal IT support resources, such as your help desk, to fielding employee questions and issues with your fax servers.

 When you move to a cloud fax model, you eliminate nearly all of these expenses, and management overhead — and replace them with a cloud service that lets you outsource all of the hardware, software, upgrades and troubleshooting to a trusted provider.

Moreover, with the right cloud fax partner you will enjoy a pay-as-you-go model where you can add or reduce fax capacity any time and pay only for what you actually use.

This is in sharp contrast to the in-house model, where you will need to make difficult binary decisions such as purchasing another fax server or additional fax lines when your capacity needs increase, even though those new resources might not be fully used, or could be under-utilized if usage declines over time.

Your Faxes Will Be More Secure
When your company deploys the right cloud fax solution, such as the eFax Corporate® system, your faxes will enjoy the most advanced security both in transit and while at rest in cloud storage. For in-transit security, your inbound/outbound faxes are immediately converted to encrypted files using the most advanced encryption protocol available— Transport Layer Security (TLS) version 1.2, which is fully compliant with HIPAA and PCI-DSS 3.1.

Of course, your faxes are in transit for only a moment or two. Then they live on forever in storage. How you protect your fax data while in storage is equally important in terms of both security and how your company stands up to your industry's regulators.

With a cloud fax partner like eFax Corporate®, your faxed data will be encrypted for secure storage in our Tier 3 or Tier 4 highly secure data centers. We keep your data backed up across multiple data centers in different geographical regions to ensure you always have access to your fax records even if one of our data centers experiences an issue.

Moreover, these data centers/colocations protect our customers' data with multiple physical and technological security measures, including:

- 24/7 onsite security personnel
- Video surveillance
- Biometric and badge access
- 256-bit advanced AES encryption to safeguard data stored on our servers
- No single points of failure for critical systems
- SSAE-16/SOC2 Type-2 Audited

In other words, the right cloud fax partner should be able to offer you the highest levels of protection for your fax data at all times — from the moment you receive or send a fax and for as long as you maintain your fax data in your cloud fax account.

Your Faxes Will Be More Compliant with Regulations
The right cloud fax system can also improve your company's alignment with your industry's regulatory requirements for data privacy and security.

The most obvious advantage of a cloud fax model over traditional faxing is that if your company receives a paper fax on an office fax machine, you are exposing any confidential and regulated data on that fax document to anyone in the

company. This includes employees, contractors, vendors and even visitors walking by — none of whom necessarily have authorization to view this confidential data. That would represent a potential gap in your compliance and could expose your company — if you were ever audited by regulators — to a penalty for compliance violations.

With a cloud fax solution, the entire fax process is handled via the web — whether through your company's email, multifunction printer, workflow application, your staff's mobile devices or through a secure web-portal. Using any of these options, you will be able to develop the protocols, the permissions and the restrictions to ensure only those authorized personnel are ever able to view or download these confidential faxes, which puts your company in a much better position with regard to your industry's data privacy regulators.

Here are some of the many ways to cloud fax.

Flexible Integration Options for Cloud Faxing
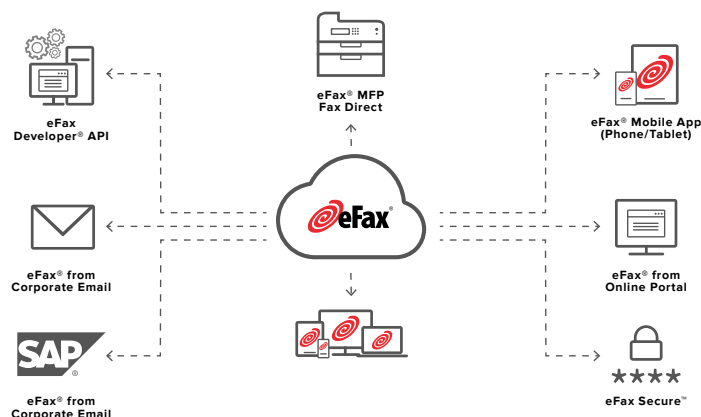
End users can send and receive faxes by email, through an online portal, from their mobile devices, multifunction printers, CRM or ERP and other productivity applications, and more.

The IT staff can even develop its own APIs to integrate eFax Corporate®'s Developer product into in-house applications and workflow platforms like Salesforce and SAP.

Why Regulated Businesses Choose eFax Corporate®

When it comes to enterprise-caliber cloud faxing, the world's most widely used and widely trusted provider is eFax Corporate®. Indeed, we for 21 years we have been the cloud fax service of choice for more heavily regulated businesses than any other company.

To cite just one example, more than half of the Top 100 Law Firms (as identified by ALM) use eFax Corporate® to send and receive their highly sensitive and confidential fax documents.

Unlike virtually every other cloud fax provider, eFax Corporate® has designed our faxing technologies specifically to comply with such privacy regulations as HIPAA, GLBA, SOX, FERPA, and similar federal, state and industry regulations.

Yet another layer of security and confidence we offer our heavily regulated customers is the fact that eFax Corporate® has been tested and certified to meet the most important security and quality assurance protocols for data protection — including ISO-27001, FIPS 140-2 and the global payment card standards body PCI-DSS.

In fact, if your organization isn't specifically regulated by one of these federal laws or private industry regulations — or if you're not sure whether your firm falls under the eye of any of these regulations — the security standards here might represent the most important metrics you'll need to judge how secure our solution is.

Of course, if you know your organization falls under regulatory oversight of a data privacy law, we would be happy to give you a walkthrough of how eFax Corporate®'s processes will help bring your faxing protocols into alignment with that law.

The eFax Corporate® Check List

✔ Our solutions are trusted by many of the world's leading businesses, in the most heavily regulated industries.

✔ We provide service to nearly half of the Fortune 500 companies worldwide.

✔ We service nearly half of the ALM Top 100 law firms — all of whom send highly sensitive information by fax.

✔ eFax Corporate® is certified for HIPAA compliance.

✔ We will sign HIPAA Business Associate Agreement.

✔ eFax Corporate® is already compliant with PCI-DSS v.3.2 encryption requirements for 2018.

✔ Faxes in transit and at rest are secured with the strongest NIST approved encryption standards – TLS 1.2 and AES 256-bit.

✔ j2 Global® owns multiple Patents on cloud and fax technology.

✔ j2 Global® has invested millions of dollars to build a secure, compliant and redundant global cloud fax network.

✔ eFax Corporate® operates on a geographically diverse global network comprised of redundant data centers and Tier III/IV rated colocations providing 99.9% server uptime.

✔ SLA for service availability and rapid Fax delivery.

✔ 24/7/365 customer support.

About eFax Corporate®

eFax Corporate® is the world's leading online fax solution, with more than 11 million customers worldwide. eFax® lets users receive, review, edit, sign, send and store faxes by email or through a web interface. eFax® offers plans for individual users and provides corporate solutions.

eFax® is a brand of the j2 Cloud Connect division of j2 Global®, Inc. and a registered trademark of j2 Cloud Services™, Inc. and j2 Global Holdings Ltd.

To learn more about outsourcing to a cloud fax model with eFax Corporate®, visit us at enterprise.efax.com

Worldwide Headquarters
j2 Global, Inc.
6922 Hollywood Blvd.
Hollywood, CA 90028

Contact US Sales:
(888) 575-7958

Email us at:
corporatesales@mail.efax.com

Web:
enterprise.efax.com

Follow Us

Please Recycle