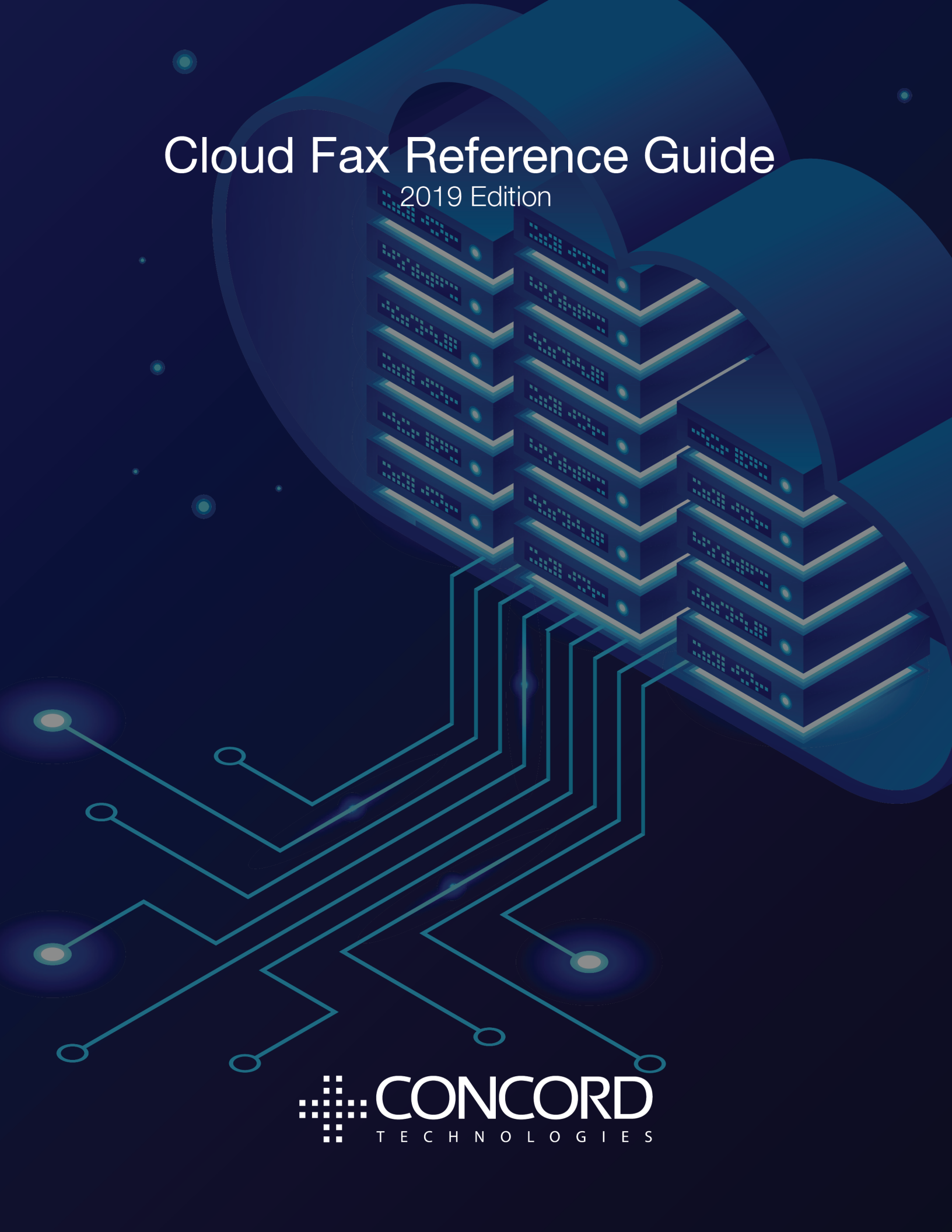
Cloud Fax Reference Guide

2019 Edition



CONCORD TECHNOLOGIES

Reference Guide Contents

Introduction

Welcome to your Cloud Fax Reference Guide

The purpose of the Cloud Fax Reference Guide is to help significantly simplify the process of scoping cloud fax platform requirements. This guide was developed by the Concord Solution Team, who have scoped, designed and implemented many of the largest global cloud-fax platforms in production anywhere on the planet today.

The Cloud Fax Reference Guide is designed for both your I.T. and business teams to use throughout the project scoping and platform selection process. The team behind the Reference Guide has taken great care to develop a tool to enable your organization to make the best buying decision, regardless of which vendor you choose.

How to use the Cloud Fax Reference Guide

This guide is separated into two sections. The first section introduces each of the individual requirements categories, and is aimed at both business and technical teams who may be in the earlier stages of their fax project. Use this section to begin understanding and identifying the requirements categories which will most impact the platform your organization ultimately selects.

The second section (The Appendix) contains a set of line-item requirements for each category. Use this section to significantly accelerate the process of developing a detailed set of project, platform and functional requirements.

Infrastructure

Your organization will want to pay close attention to each vendor's availability, deliverability and security provisions to get a full picture of their cloud fax network's infrastructure. The cloud fax infrastructure impacts every aspect of the service. Getting it right will provide your organization with a low maintenance, reliable service where users can send and receive faxes quickly and efficiently even in cases of data center, network or telecom outages. Getting it wrong can dramatically inflate the risk of downtime and delivery failures, while further taxing I.T. bandwidth.

What is availability?

Availability relates to a fax provider's ability to maintain network and service operation in the event of a technical failure or unforeseen disaster. Availability also covers the ability of that system to continue providing access to user tools, applications and portals.

Vendor definitions of availability or high-availability vary greatly. For instance, while most fax service providers promote a high-availability architecture, few operate networks designed to ensure uninterrupted operation when network, data center or telecom issues arise.

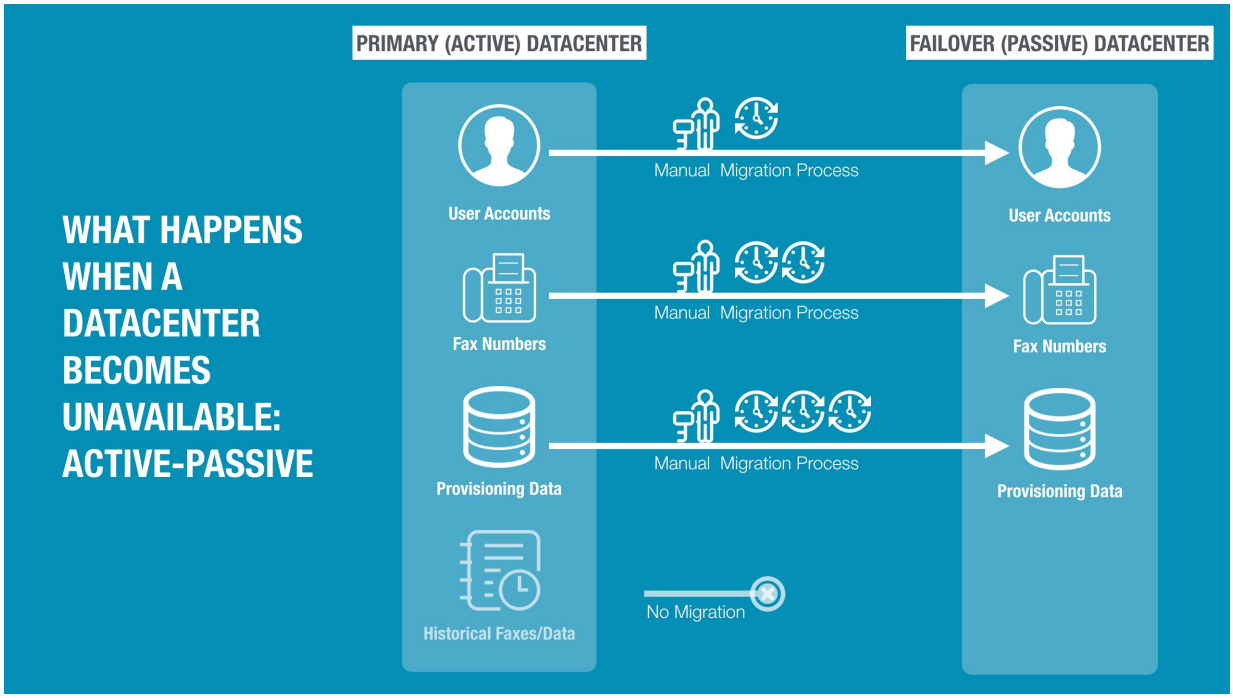
Data center configuration

Most (if not all) enterprise-grade fax services run on high availability networks which harness multiple data centers to process fax traffic. While fax buyers are frequently tempted to evaluate cloud services based on the number of data centers in a network, it is the configuration of those data centers that ultimately determines the service's ability to remain online and operational should infrastructure problems arise. For instance, a network comprising two data centers configured as "active-active" provides significantly more resilience than six or even eight servers set up in a legacy "active-passive" model.

Active-Active vs. Active-Passive fax networks

The difference between Active-Active and Active-Passive is that the former utilizes multiple data centers simultaneously to process any and all fax traffic. Active-Active networks do not rely on a failover process to switch traffic or customers to an alternative location when an issue arises.; all components in an Active-Active architecture are working seamlessly together regardless of physical location.

By contrast, an Active-Passive architecture requires a (typically manual) failover process to migrate telecommunications, user accounts, old fax images and other configuration items over to a new location when the primary location experiences issues. Users of a fax service (or any cloud service for that matter) built on an Active-Passive architecture are typically unable to access the service while the failover process takes place. How long the failover process takes varies greatly, but it's not uncommon for users to be locked out for hours or in serious cases, days.



Data center compliance

Organizations seeking a fax service which complies with specific regulations should seek confirmation that all the data centers within a fax service provider's network are compliant. In some cases, the primary servers (found in active-passive fax networks) are compliant but the failover (back-up) servers are not. In other cases, the failover servers may even be located in other countries, potentially presenting serious challenges with data sovereignty.

What is deliverability?

Whereas availability refers to a fax service provider's ability to ensure the service is always operational, deliverability refers to the provider's ability to successfully transmit faxes in a timely manner.

For organizations using outbound fax in core business processes, successful and timely delivery of fax messages consistently ranks as a chief concern. Maintaining a high throughput and deliverability rate requires fax service providers to effectively process requests, dial fax numbers and terminate faxes across a wide range of devices, protocols, carrier networks and destination countries.

Understanding how providers plan and manage the system, network and carriers which impact deliverability will enable you to identify providers who may be a good match. Spotting potential service issues will also become much easier.

Infrastructure | Deliverability | Telephony

For this guide, the term “deliverability” will be used to cover the successful transmission of both inbound and outbound faxes. For most fax service buyers, deliverability is equally as important as availability, as shortcomings in either immediately impact business processes.

Telephony technology

Telephony is possibly the most critical factor in determining a fax service provider’s ability to supply you with a service which meets your deliverability needs.

Providers typically rely on two primary technologies for sending and receiving faxes: TDM (Time-Division mMultiplexing) and FoIP (Fax over IP or Internet Protocol). Both of these technologies have their own strengths and weaknesses, depending on their implementation.

TDM (Time-Division Multiplexing)

TDM is the pre-IP standard for telephony. For the purpose of this guide, “TDM” will be used as a general term to include traditional TDM as well as T1, E1, DS3 and similar digital services which are not IP-based. TDM lines are owned and managed by telecom carriers.

TDM Strength: While TDM may be considered “legacy” it is typically the most reliable and efficient method for transmitting outbound faxes. TDM is less susceptible to potential compatibility issues with the fax hardware used on the recipient’s end. Unlike its IP-based counterpart, FoIP, TDM’s technology does not suffer from packet loss issues.

Weakness: As strong as TDM is for outbound, it is a less attractive prospect for inbound fax delivery. Unlike FoIP, a TDM line can only be connected to a single data center. If the data center becomes unavailable, there is no simple way to automatically reroute the fax to another data center. Fax delivery will continue to fail until the data center issue is resolved or the telecom carrier reroutes the affected fax number(s) to an alternative circuit connected to the backup datacenter. This process is time consuming, error-prone and in many circumstances, not even feasible at all.

FoIP (Fax over IP)

FoIP (Fax over IP) delivers faxes digitally, over packetized networks using IP rather than analog TDM circuits.

FoIP Strength: Unlike TDM, FoIP is not tied to a single data center. Inbound faxes can be routed to the destination via any available data center. If one data center becomes unavailable, the fax is automatically routed via another. This makes FoIP a far more reliable option for inbound fax delivery compared with TDM.

Weakness: FoIP is more susceptible to potential compatibility issues with the sender's hardware. FoIP is also susceptible to packet loss which makes it a little less robust than TDM.

Getting the telephony mix right

As the title suggests, using a pure-play TDM or FoIP approach for fax delivery creates a number of potential issues. Compared with TDM, FoIP is far less expensive to implement and maintain, making it popular with many cost-conscious fax service providers. Unfortunately, services which rely heavily on FoIP often struggle to meet end-user expectations for deliverability and efficiency.

The optimal approach consists a mix of TDM for outbound delivery and FoIP for inbound. TDM's superior outbound performance plays well alongside FoIP's inbound routing flexibility. This flexibility significantly outweighs FoIP's compatibility and packet loss issues, and typically results in far higher inbound call completion rates compared with TDM.

Telecom carriers

Fax services utilizing TDM will process calls using one or more carriers. Each carrier has its own strengths and weaknesses when it comes to successful call completion. In many cases, this is regional, with some carriers faring better than others, based on where the fax will be ultimately delivered to. Individual carriers are also susceptible to regional outages and service degradation. By contracting with multiple carriers for outbound, fax providers are able to increase their ability to consistently deliver calls across all regions. By utilizing multiple outbound carriers, fax providers can (or at least should) develop routing strategies which continuously leverage carrier performance to automatically select the best carrier in each delivery scenario.

The “call completion” rate is the primary metric used to determine how consistently a fax service provider successfully delivers faxes to their destination. Vendor call completion rates are, however, rarely publicized and vendors are typically inconsistent in their willingness to share this data.

When call completion rates are shared by a vendor, it’s important for your organization to understand what goes into those numbers and how much weight to give call completion in the evaluation process.

Apples-to-apples comparisons are challenging; there is no standardized method for determining call completion rates. Most fax service providers will control for certain performance variables such as busy signals or dial attempts to non-fax numbers. These controls can lead to dramatically different numbers from vendor to vendor. While it may be difficult to normalize vendor numbers for comparison, your organization should, at very least, understand how the numbers were generated.

Your own mileage may vary. Where you send faxes to and receive faxes from impacts your own call completion rate. This is especially true with international sources and destinations. Expecting your own results to mirror your vendor’s numbers may be unreasonable. This is why it’s vital to understand how those vendor call completion rate stats were generated.

Trust and verify: The only practical method for verifying call completion rates is to use the service. Most organizations focused on outbound delivery performance will pilot one or more services, either sequentially or in parallel. We recommend you do the same.

There will always be instances where a fax is not delivered to the recipient. This can be caused by a variety of factors, ranging from carrier network outages to poor line quality, or compatibility issues between inbound and outbound fax hardware. How each platform addresses undelivered faxes will impact both call completion rates and delivery time.

Vendor approaches to call optimization and error handling vary greatly. At a minimum, you should understand:

1. What happens when a fax is not delivered?
2. Can the fax service adapt its delivery method, once a failed delivery is encountered?
3. Can the fax service optimize delivery by re-routing faxes to avoid “black spots”?

What happens when a fax is not delivered?

Buyer requirements here broadly fall into one of two buckets: “keep trying” or “stop and tell me.” The “keep trying” approach often works for the delivery of faxes which don’t need to arrive within a very short time frame. This method enables the fax service to retry the call multiple times with the expectation that the fax will ultimately be delivered. The “stop and tell me” approach is used for time-sensitive transactions. Should the fax fail, the sender needs to know immediately so they can use another method to deliver the information. Online food delivery services using fax to send customer orders to restaurants operate within tight time frames, so they don’t have the luxury of waiting for the fax service to make multiple delivery attempts.

Understanding how fax delivery impacts your business processes will help you determine how you will need to respond to delivery issues.

Can the fax service adapt its delivery method, once a failed delivery is encountered?

While some deliverability issues can be resolved simply by retrying the call, more persistent issues, such as network, carrier or compatibility issues often require the fax to be transmitted in a different way or by using a different route to the destination.

Can the fax service optimize delivery by re-routing call paths to avoid “black spots”?

Proactively optimizing call paths around persistent choke-points will reduce the number of retries, providing improved call completion rates and delivery time.

Infrastructure | Security

Security should be high on the priority list for any organization sending or receiving sensitive, confidential or proprietary information, in particular, those operating in regulated environments (note, this document provides a dedicated section for compliance). This section breaks down security requirements into three parts: physical, network, and application.

Security | Physical Security

This section covers the measures in place to protect the fax platform's hardware, software, networks, data and personnel from physical attacks and natural disasters, both of which can render the data center inoperable and/or permanently destroy provider and customer data.

Security | Network Security

This section covers the measures in place to protect the fax platform's network infrastructure from unauthorized access to its systems, software or data. While each of the security elements are critical, fax platforms with ineffective network security invite the widest range of external attacks.

Security | Application and Logical Security

This section covers the measures in place to protect the fax platform's applications and underlying operating systems. Unauthorized access to provider applications can result in the distribution, modification or destruction of fax provider and customer data. Unlike physical and network security measures, application security is handled as part of the application development process, making it part of the platform's DNA.

Application and System Integration

As your organization evaluates cloud fax services, consider the ways in which that service will need to be integrated into your existing systems. Cloud fax providers which are able to integrate into your operations via API or web services may make it easier to seamlessly embed fax capabilities into your core systems and processes.

Integration | API / Web Services

The tightest and most functionally sophisticated integrations are created using the fax service provider's API. Custom-coded integrations typically far exceed the capabilities associated with the other integration options and provide a seamless user experience. While organizations which opt for an API integration may incur higher initial implementation costs compared with other approaches, the return on investment is frequently higher and realized more quickly.

Integration | Application Connectors

Application connectors function much like desktop plug-ins, but are generally integrated with fax at the server level. As an example, a vendor may offer a connector for Microsoft CRM. Once implemented, all permitted users would be able to send and/or receive faxes using their MS CRM client or web application. Application connectors provide a great deal of convenience by eliminating the need to custom code an integration between the fax platform and target application/device. The reliability and capabilities of each application connector often wildly differ between vendors. Furthermore, plug-ins produced by a single vendor can be highly variable in terms of reliability and capabilities. For instance, a vendor may offer a rich and robust fax connector for EHR Application "A," but far more limited and error-prone connector for EHR application "B." It is also not uncommon for vendors to reduce their development investment in a connector over time, which may lead to delays in supporting new versions or features of a platform. Look at each vendor's long term track record with the connectors they offer.

Capabilities

Capabilities | System Capabilities

The more ways a cloud fax provider can enable your organization to send and receive faxes, the easier it is for users to utilize the service. Assessing a provider's system capabilities will give your organization insight on how flexible you can be when it comes to harnessing existing systems or implementing new ones. These requirements can also shed light on ease of use questions, like what kinds of file types are supported, or whether the provider offers services like a web portal or address book functionality. This section will allow your organization to assess the system capabilities that give you flexibility and control over how you send and receive faxes.

Capabilities | User Capabilities

A cloud fax provider's available user capabilities should allow members of your organization to customize their own fax experiences. These customizations could be as specific as choosing how an individual user's signature is displayed on a sent fax, or as broad as impacting how that user can interact with and view received faxes. The more a user can customize his or her own experience, the more a cloud fax provider's platform can be utilized in a manner that is specific to each individual's role.

Capabilities | Administration Capabilities

A cloud fax provider that offers a wide range of administrative capabilities within their service is especially helpful for large organizations that have many fax users. For instance, functions like being able to set user privileges according to an organizational hierarchy make it easy to manage a high volume of users. For some organizations, it's also important for administrators to be able to make changes on a self-serve basis, without needing to contact the fax service provider. If this kind of agility is important to your organization, admin functions like the ability to control fax number inventory or initiate number porting without contacting the vendor will be crucial.

Capabilities | Tracking and Reporting

Tracking and reporting plays a key role in any enterprise organization. Basic tracking and reporting should enable I.T. teams to keep track of common fax activity and costs.

Businesses operating in more highly regulated industries will need more advanced tracking reporting, designed to provide insight into fax-centric business processes. Regardless of where your needs fall, the target fax service should provide the means to quickly tap into those data-points.

Compliance

The kind of information your organization creates, accesses, distributes or retains determines which standards and regulations you will be impacted by.

If you are currently using fax machines, fax servers or fax appliances, your organization typically assumes all the compliance risk. Moving to a cloud-based provider should enable your organization to transfer some of that risk over to the provider.

Use the following compliance sections to learn how each regulation impacts your faxing requirements and the providers you evaluate.

Compliance | Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Highlights	
Compliance certification / validation process	None
Certification/validation expires	Not Applicable
Certification/validation documentation	Not Applicable
Minimum documentation vendor should provide	HIPAA Business Associate Agreement (BAA)
Additional documentation vendor should provide	Fax Service Provider - Service Level Agreement

Given that HIPAA compliance is essential for any organization handling protected health information (PHI), it's unsurprising that it exists as a core requirement for fax service buyers. It's equally unsurprising that almost every enterprise-grade fax service provider promotes their fax service as being HIPAA-compliant.

Until recently, no formal HIPAA audit process existed. This changed when, in March of 2016, the OCR (Office for Civil Rights) introduced the Phase 2 HIPAA Audit Program. For detailed information on the audit process click here.

What you need to know about the Phase 2 HIPAA Audit Program

1. The audit process is still a work in progress. The last round of updates to the process were announced in July of 2018. Affected organizations can expect to see these audit requirements evolve over time.
2. Audits are currently optional for both covered entities and service providers. Those who wish to be audited may "opt-in" with the OCR ultimately selecting who will participate in the program.
3. Going forward, we expect to see an uptick in buyers enquiring about HIPAA-audited fax service providers, as the program becomes more established.
4. Few fax service providers have undergone the audit process as of the time this guide was published.

How to effectively evaluate Fax Service Providers for HIPAA Compliance

Verify the scope of HIPAA compliance.

A minimum of three organizations work in concert to send and receive your faxes: The fax service provider, the data center provider and one or more telecom providers. HIPAA mandates that each of these entities meet the required standards (where applicable). For example, evidence that a fax service provider's data center is HIPAA compliant is meaningless if the fax provider itself is not.

Get past "HIPAA Compliant."

While it makes sense to narrow your list of potential fax service providers down to those who claim to be "HIPAA Compliant", it is crucial to evaluate how each of them meets the specific Code of Federal Regulations (CFR) set forth in:

- 45 CFR §164.308 - Administrative Safeguards
- 45 CFR §164.310 - Physical Safeguards
- 45 CFR §164.312 - Technical Safeguards
- 45 CFR §164.316 - Other Security Controls

Identify circumstances that may compromise or even inhibit compliance with the standard.

Highly "edited" vendor positioning statements around compliance can quickly mislead buyers. For instance, a provider's primary data center being HIPAA compliant in no way guarantees their secondary data centers are also compliant. In the case of a failover, you may discover the vendor's backup data center is far from HIPAA compliant. Draft requirements that prevent service providers from making broad generalizations about their fax network infrastructure; if in doubt, get specific.

Check a vendor's track record.

Ensure target vendors provide detailed information on any previous compliance breaches, audits or issues.

Eliminate "conduits" from your evaluation process.

If a vendor claims they are exempt from HIPAA due to the "conduit exception" — move on. Reference the section on HIPAA Conduit Exceptions for more information on this topic.

Ensure your fax service provider is qualified to sign a Business Associate Agreement (BAA).

Many fax service customers enter into BAAs with a fax service provider assuming the vendor is fully cognizant of the agreement's scope and risks. Unfortunately, many vendors enter into the agreement with limited understanding of its impact, or assume that their security provisions automatically meet the requirements.

Given that it's the covered entity which is ultimately responsible for complying with HIPAA, here are the best practices for evaluating a vendor's ability to meet the terms of the BAA:

1. Seek out vendors which do not attempt to mitigate their risk by limiting the scope of remedy or assumed liability in the BAA.
2. Vendors which are unable to show how their service directly meets the requirements for each CFR should be avoided.
3. Focus on vendors capable of demonstrating a thorough understanding of HIPAA. This should be backed up with evidence of a formal training program for the service provider's employees.
4. Avoid vendors which take a reactive approach to changes in the regulation. Your chosen vendor should be ahead of you when it comes to supporting requirements.

Evaluate your own processes centered around faxing.

A compliant fax service is rendered immediately ineffective when implemented within processes with little information governance. For instance, a securely delivered fax is no longer secure if it is printed and left on the receptionist's desk for other patients to view. Consider the paths PHI documents take before and after fax transmission.

PCI DSS Highlights	
Service providers processing **more than 300,000** accounts/transactions annually.	
Compliance certification / validation process	Annual on-site security audit performed by Qualified Security Assessor (QSA).
Certification/validation expires	Every Year
Minimum documentation vendor should maintain	1. Report on Compliance (ROC) completed by QSA 2. Network Scan by Approved Scan Vendor (ASV) for last four quarters 3. Attestation of Compliance form (AOC) 4. Annual Penetration Test
Service providers processing **less than 300,000** accounts/transactions annually.	
HIPAA compliance certification / validation process	Vendor completes self-assessment questionnaire. (SAQ)
Certification/validation expires	Every Year
Minimum documentation vendor should maintain	1. Annual Self-Assessment Questionnaire (SAQ) 2. Network Scan by Approved Scan Vendor (ASV) for last four quarters 3. Attestation of Compliance form (AOC) 4. Annual Penetration Test

Organizations that are subject to PCI DSS compliance will need to ensure that the cloud fax service provider they use is also PCI DSS compliant. Unlike HIPAA, verifying PCI Compliance is a straightforward process. Fax service providers transmitting more than 300,000 credit card transactions per year are required to undergo a third-party audit. Those who process less than 300,000 are required to complete a self-assessment questionnaire known as the SAQ. PCI Compliance also mandates vendors to submit to a number of network security tests (all of which is covered in the Appendix section).

Best practices for evaluating PCI-Compliant fax service providers.

Verify the scope of PCI compliance.*

A minimum of three organizations work in concert to send and receive your faxes; the fax service provider, the data center provider and one or more telecom providers. You will need to verify that BOTH the fax provider and the data center provider are PCI compliant. As far as the telecom provider is concerned, they should be out-of-scope so long as they are offering nothing more than a circuit for the fax transmission.

Verify compliance documentation is valid.

PCI compliance expires after a year and many of the supporting tests must happen quarterly. Ensure the documentation you receive from the vendor is up to date.

Check the vendor's track record.

Ensure target vendors provide detailed information on any previous compliance breaches, audits or issues.

**excludes on-premise environments.*

Compliance | SSAE-16 SOC 2

SSAE-16 SOC 2 Highlights	
Compliance certification / validation process	Vendor undergoes audit by qualified third party auditor.
Certification/validation expires	Every year
Minimum documentation vendor should provide	SSAE-16 SOC2 Certificate SSAE-16 SOC2 Report
Additional documentation vendor should provide	None

Unlike HIPAA and PCI DSS compliance, SSAE-16 SOC2 isn't content-specific (think protected health information, a.k.a medical records) or transaction-specific (think credit card transactions). SSAE-16 SOC2 is designed to:

"Protect the security of an organization's financial and computing resources, as well as personal information transmitted or stored by the organization."

SSAE-16 SOC2 comes into play if a) your organization is SOC2 compliant and therefore limited to using other SOC2 compliant vendors or, b) your organization has elected to use SOC2 as the template for evaluating vendor security and privacy standards.

Evaluating a potential fax service vendor's SOC2 compliance is as simple as requesting their current SSAE-16 SOC2 certificate or the more detailed report. Both the certificate and report can be useful to assess the overall maturity of the vendor's information security posture, and to ensure a thorough third party audit has been performed to validate the vendors claims or intentions.

Best practices for evaluating SSAE16 SOC2-Compliant fax service providers.

Verify the scope of SOC2 compliance.

It is not uncommon for fax service buyers to ask for SOC2 documentation only to be furnished with the data center's SOC2 certificate. SOC2 certificates must be provided for both the data center and the fax service provider itself. Receiving just the data center certificate should serve as a red flag, as a datacenter provider's SOC2 certification has no bearing on the processes, procedures and technical measures of the fax vendor itself.

Verify compliance documentation is valid.

SOC2 compliance expires annually, so ensure all documentation is up-to-date.

FedRAMP Highlights	
Compliance certification / validation process	Vendor undergoes assessment process in accordance with the Federal Information Security Management Act (FISMA)
Certification/validation expires	Every three years
Minimum documentation vendor should provide	FedRAMP Security authorization package documentation

While major Infrastructure-as-a-Service vendors such as Amazon Web Services, Microsoft, HP and IBM have embraced FedRAMP, most cloud service providers have yet to become FedRAMP-compliant. Given FedRAMP's current requirements, it's unlikely that fax service providers will be particularly different.

For government organizations which are limited to using FedRAMP authorized services, there are currently three possible approaches:

1. Implement an on-premise fax solution. An on-premise solution negates the requirement for FedRAMP, but forces the organization to implement and maintain their own server and telephony infrastructure —something most are actively seeking to avoid.
2. Seek a waiver to operate a non-FedRAMP compliant service —although there is no guarantee the waiver will be granted.
3. Leave the existing fax infrastructure as-is.

Vendor Support

Vendor Support | Implementation and Training

For large organizations with many fax users, finding a cloud fax service that's simple to implement will go far in fostering quick adoption and reducing loss of productivity. The ideal cloud fax provider for your large organization should integrate seamlessly into existing systems and offer user-friendly interactions.

Vendor Support | Customer Support

The right cloud fax provider will ultimately want your business to succeed with their cloud fax service, and will offer support and services to foster that success. Not only will the ideal cloud fax provider support your efforts, they won't lock your organization in with extreme service contracts or sky-high fees to terminate the agreement. A cloud fax service provider with an outstanding product and service won't need to worry about locking customers in with ironclad contracts; the quality of service will stand on its own.

Appendix

Appendix A - Infrastructure: Availability Requirements

Appendix B - Infrastructure: Deliverability Requirements

Appendix C - Infrastructure: Security Requirements

Appendix D - Application and System Integration Requirements

Appendix E - Capability Requirements

Appendix F - HIPAA Compliance Requirements

Appendix G - PCI DSS Compliance Requirements

Appendix H - SSAE-16 SOC2 Compliance Requirements

Appendix I - FedRAMP Compliance Requirements

Appendix A - Infrastructure | Availability Requirements

General Availability Requirements

1. What is the maximum peak fax volume supported by the current inbound faxing infrastructure?
2. What is the maximum peak fax volume supported by the current outbound faxing infrastructure?
3. What percentage of peak available capacity is currently being utilized (last 90 days)?
4. How many primary data centers would be used to service clients' Cloud Fax traffic and, if more than one, then how do they share traffic load?
5. How many secondary/failover data centers would be used to service clients' Cloud Fax traffic?
6. List all data centers and please indicate:
    a. Whether the data center is primary or secondary for our expected traffic
    b. The data center location
    c. The data center vendor
    d. The telecom carriers the data center connects to
    e. What traffic capacity considerations, if any, are there at each location

Availability | Failover / Disaster Recovery Requirements

1. Please provide a copy of your Business Continuity and/or Disaster recovery policy.
2. Please describe your Recovery Time Objective(s) (RTO).
3. Describe, in detail, the decision and physical processes for failover in case of a problem with primary service location / servers.
4. How are customers notified of a failover situation?
5. How many times has a failover situation affecting more than one customer occurred in the last twelve months?
6. For each failover situation, describe the reason, scope, time to resumption of services and final time to resolution.
7. Please describe your Service Level Agreement (SLA) policy for service uptime.
8. What is the SLA's guaranteed minimum uptime %?
9. How many times has the service failed to meet the uptime SLA in the last twelve months?
10. Do contracts include a penalty or remediation clause for breach of availability and continuity SLAs?

Availability | Infrastructure Maintenance and Investment

1. Is there a scheduled maintenance window which results in client downtime? If yes, what is the scheduled maintenance window, maximum allowable downtime and required notification period?
2. Please describe the process used to ensure clients are notified prior to changes being made to the fax platform which may impact their service (whether expected to be service interrupting or not).
3. Please list all unplanned maintenance over the last twelve months which resulted in the platform being unavailable for one or more customers.
4. Please list all currently identified maintenance to the fax network planned in the next twelve months which will result in the platform being unavailable for one or more customers.
5. Please list all major fax network infrastructure investments made in the last 24 months.
6. Please list all major fax network infrastructure changes planned in the next 24 months.

Appendix B - Infrastructure: Deliverability Requirements

Deliverability | Partial Page and Failed Transmission Requirements

1. Please describe how the platform processes partial/incomplete inbound faxes.
2. How are users and administrators notified of partial inbound faxes?
3. How are users and administrators notified of the failed outbound faxes?
4. In the event that delivery of an outbound fax fails, what measures does the platform take to increase the likelihood of a successful transmission on redial?
5. What technologies/techniques/methods are used to optimize inbound page completion rates?
6. What was the call completion rate for all outbound calls on your platform in the last calendar month (defined as all calls placed which were initially answered by fax tone)?
7. What is the call completion rate for inbound calls (defined as percentage of all calls where a complete end-of-transmission signal was received, indicating that the call terminated normally)?

Deliverability | Telephony Requirements

1. Please describe the telephony technologies used for outbound faxing (SIP, T.38, G.711, TDM, etc.).
2. If more than one technology is used for outbound faxing, please describe what determines when one technology is used over other(s).
3. Please describe the telephony technologies used for inbound faxing (SIP, T.38, G.711, TDM, etc.).
4. If more than one technology is used for inbound faxing, please describe what determines when one technology is used over the other(s).
5. Which telephone carrier(s) does the fax platform utilize for outbound faxing?
6. Which telephone carrier(s) does the fax platform utilize for inbound faxing?
7. What is the process for porting a customer's existing set of fax numbers to the fax platform?
8. How long does the porting process take?
9. Please describe the process and all restrictions in place for porting fax numbers away from your service, to a different provider.
10. Describe capabilities for provisioning and porting international numbers.
11. What is the anticipated downtime, if any, associated with activation of service and the porting of numbers to vendor?

Appendix C - Infrastructure: Security Requirements

Security | Physical Security Requirements

1. Where are the data center(s) located?
2. For each data center:
    a. How is employee access to the data center controlled?
    b. How is employee access to the data center monitored?
    c. What background checks are performed on employees prior to being granted authorization to the data center?
    d. Please list all known third parties who potentially have access to the data center (such as backup vendors, service providers, equipment support maintenance, software maintenance vendors, data recovery vendors etc.)
3. For each third party, please describe:
    a. The functions the third party will carry out at the data center.
    b. Which systems, applications and services the party has access to.
    c. Frequency of third party's visits to the data center.
    d. Background checks performed on third party representatives prior to being granted authorization to the data center.
4. Are visitors permitted in the facility?
5. How is visitor access logged and controlled?

Security | Network Security Requirements

1. Are firewalls in use for both internal and external connections?
2. How frequently are vulnerability assessments performed on internal and production cloud fax networks?
3. How frequently are security scans performed on internal and cloud fax networks?
4. How frequently are penetration tests performed on internal and cloud fax networks?
5. Please describe the process of updating/patching the cloud fax network security.
6. Please describe how users are technically prevented from accessing the fax platform via non-managed private devices.
7. Are documented procedures in place describing the control processes over network security and administration processes?
8. Are network and host intrusion detection and prevention (IDS / IPS) systems in place?
9. If so, please describe when and how they are deployed.
10. What processes are in place to systematically audit and review:
    a. Access attempts
    b. Security events
    c. Firewall logs
    d. System logs
11. Describe the alerting and response process used in the event the Intrusion Detection System detects a suspicious event or exceeds normal thresholds for your environment.
12. Does vendor allow remote access to platform and if so, how is this secured?
13. Are third party contractors and personnel capable of accessing the production cloud fax network and if so, how are connections secured and privileges managed?

Security | Application and Logical Security Requirements

1. Are security engineering principles embedded into the System/Software Development Lifecycle (SDLC) to achieve the goal of "secure by design" when designing, building and updating systems?
2. Please describe what options are available to fax customers to specify where their data will be stored.
3. Please describe what options exist for customers to specify the duration of fax document storage. Can fax documents be deleted immediately?
4. How is fax data encrypted during transit?
5. How is fax data encrypted while at rest?
6. How are encryption tools managed and maintained by the cloud fax network?
7. How are users and administrators authenticated on vendor platform?
8. Does the service support minimum password standards for length, complexity, characters, etc.?
9. Are controls in place to protect the authenticity of communications sessions?
10. How are archived faxes encrypted?

Appendix D - Application and System Integration Requirements

Integration | API / Web Services Requirements

1. Please describe the API platform protocols (e.g. SOAP, REST, other).
2. Please describe the application/web services API's core sending capabilities.
3. Please describe the application/web services API's core receiving capabilities.
4. Please describe the application/web services API's core user management / admin capabilities.
5. Please describe the application/web services API's core individual job and job batch reporting capabilities.
6. Please describe the application/web services API's ability to generate tracking/reference IDs for job tracking through fax transmission.
7. Please list all major enhancements to the application/web services API planned for release in the next twelve months.
8. Please describe the available developer documentation for sending and/or receiving faxes programmatically via application/web services API.
9. Please describe the code samples available for developers.
10. Is developer support available?
11. Please describe the scope of that support.
12. How are developer support resources accessed?
13. Is there a cost associated with gaining access to coding resources, documentation and/or developer support?
14. What is your average time to first dial for outbound faxes submitted by API? Is this time period defined in your SLA?
15. What is your average delivery time for inbound faxes to API destinations? Is this time period defined in your SLA?

Integration | Other

1. Does the platform support the use of shared or network folders for the purpose of sending faxes? If supported, please describe how this is facilitated.
2. Does the platform support the use of shared or network folders for the purpose of receiving faxes? If supported, please describe how this is facilitated.

Appendix E - Capability Requirements

Capabilities | System Capability Requirements

Email-based Faxing

1. Please list the email platforms that the service supports for email-to-fax (Desktop, Web and Mobile).
2. Please describe the capabilities of any fax plug-ins or clients for particular email applications (Desktop, Web and Mobile). What deployment methodologies are supported for these plug-ins? What email client application versions are supported?
3. Please describe the notifications and associated options available to email-to-fax users.
4. What file-types are supported for the delivery of inbound faxes to email?
5. Do you support Searchable PDF delivery for inbound faxes to email? Is there an additional cost for this?
6. What is your average time to first dial for outbound faxes submitted by email? Is this time period defined in your SLA?
7. What is your average delivery time for inbound faxes to email destinations? Is this time period defined in your SLA?
8. Describe how an outbound user, sending a fax via email, can edit transmission for coversheet details and other fax related settings such as scheduling, tracking and reporting.
9. Can inbound faxes be directed to more than one destination type (e.g. email and FTP simultaneously)? If so, what are the options?

Desktop Faxing

Please indicate how each of the following desktop faxing use cases are supported:

1. Fax from any application offering a print function (similar to PDF print drivers). How are status and notifications communicated to the user in this model?
2. Convert an unsupported file type to a supported file type for faxing.
3. Fax document captured using an attached desktop scanner.

Faxing via Multi-Function Print (MFP) Devices

1. Does your solution support faxing from MFPs? If so, please respond below:
2. Does your solution utilize native client applications for MFPs? If so:
    a. Please provide a detailed list of makes and models supported and identify any functional limitations or dependent software and features for the support of each.
    b. Please describe the licensing model and how fleet refreshes or fleet migrations (new manufacturer) are handled.
3. If you do not utilize native client applications for MFPs, then please describe the interface options available to users and the transport /integration protocols used.
4. Please indicate how each of the following MFP faxing use-cases are supported:
    a. Outbound fax - no user authentication required at the device.
    b. Outbound fax - user authentication enforced at the device.
    c. Outbound fax - automatic printing of delivery confirmations by the MFP device.
    d. Outbound fax - send delivery confirmation to sending user via email.
    e. Outbound fax - track/report fax activity at the device level.
    f. Outbound fax - track/report fax activity at the user level.
    g. Inbound fax - automatic printing of faxes at device for all users.
    h. Inbound fax - faxes delivered directly to recipient's email inbox.
    i. Inbound fax - track/report fax activity at the device level.
    j. Inbound fax - track/report fax activity at the user level.

Inbound Fax Routing

1. How and to what extent are each of the following supported?
    a. Assign inbound faxes to a specific user.
    b. Assign inbound faxes to teams/departments/groups of users.
    c. Assign inbound faxes to a specific business process or queue.

Address Book Management

1. Please indicate which of the following are supported:
    a. Access corporate or shared address book of fax recipients.
    b. Create and manage local address book of regular contacts.

File Type Support

1. Please list all file types natively supported by the platform for outbound faxing and define any usage limitations related to the file types listed above.
2. How does the fax platform respond to attempts to send non-supported file types?
3. What are the file size and or maximum pages supported by the platform?

Capabilities | User Interface Requirements

User Interface Definition:

1. Briefly describe what user interfaces are available for users to interact with their faxes (Web, Windows, MacOS, Android, IoS, other).
2. What is the recommended maximum size (number of) faxes supported in each client or folder / inbox before performance is negatively impacted?

For each of the sub-sections below, please indicate:

1. Whether or not the capability is supported.
2. Which interfaces are supported (desktop, web, mobile, other).

Basic View and Search:

1. View inbound and outbound faxes.
2. Filter view based on fax status (sent, resent, failed, received, partial etc.)
3. Receive audible notification of inbound fax arrival.
4. Filter view based on tag or metadata value.
5. Search for faxes based on basic metadata (fax number, date of transmission etc.)
6. Search for faxes based on tag or other metadata value.
7. Search for faxes based on text content of the faxes.

Outbound faxing

1. Create a personalized fax cover page.
2. Attach and sort multiple documents to a fax.
3. Specify recipient details beyond fax number, such as name and company.
4. Send a single fax to multiple recipients.
5. Use mail-merge style functionality to send personalized fax to list of external fax recipients.
6. Forward / route faxes to other internal users or groups of users.
7. Assign additional tracking information to fax for reporting purposes (tracking numbers, recipient information, re-billing information etc.)
8. Resend a fax directly from web portal or dashboard.

Inbound Faxing

1. View an inbound fax.
2. Rotate fax pages (correct upside-down faxes).
3. Add/modify/remove custom information pertaining to a fax (e.g. capture patient name and referring physician).
4. Forward / Route received fax to other users or groups.
5. Delete faxes.
6. Archive faxes.
7. Delete one or more pages from a multi-page fax.
8. Split a single multi-page fax into multiple documents.
9. Annotate / add text to a fax.
10. Redact area(s) of a fax.
11. Erase area(s) of a fax.
12. Add a digital “stamp” to a fax.
13. Digitally sign fax documents (include description of capabilities and whether solution is compliant with ESIGN act).
14. Describe the logging and audit trails maintained for any and all user interactions with faxes in their inbox and how these are available to the users and to administrators for audit purposes.
15. Describe how / which of these capabilities can be enabled or disabled for users (disable the ability for user to delete fax).

Team / Departmental workgroups

1. Assigning faxes to individual teams / groups or queues.
2. Which user within the department is working with / last worked with a specific fax document.
3. The time elapsed for the fax to be actioned by a user in the workgroup.
4. The current status of a particular fax within the workgroup.
5. Describe the audit trails / history information available to team managers to view interactions of their team members with individual faxes.

Capabilities | Administrator Requirements

1. Describe manual processes for administering users and performing moves, adds, changes and deletions on the fax user base.
2. Describe automated processes for administering users and performing moves, adds, changes and deletes on the fax user base.
3. Does the solution support Active Directory / LDAP integration for provisioning?
4. Does the solution offer an API for account management functions?
5. Does the fax solution support organizing users into groups? If so:
6. Can groups be organized into a hierarchy for administrative access at the group level? If so:

    6a. How deep can groups and sub-groups be nested?

    6b. How are new users notified of their account status and fax number?
7. Does the solution support role-based access and permissions for administrators? If so:

    7a. Describe the features and functions that can be enabled / disabled for an administrator.

    7b. Describe the process to requisition new fax numbers, domestic and international.

    7c. Describe the process to manage adding and editing cover pages.

Capabilities | Tracking and Reporting Requirements

1. What standard reports are offered by your solution?
2. Can users create and store / reuse custom reports?
3. Can users create custom filters for reports?
4. Are real-time reports available or is reporting based one historical data (how old?)
5. What tools are available to view inbound/outbound fax activity by user or group?
6. What tools are available to view total usage trends and identify trend deviations?
7. What SLA performance reporting is available?
8. Provide details of outbound call completion research and analysis available.
9. Provide details of inbound call outcome research and analysis available.

Appendix F - HIPAA Compliance Requirements

HIPAA Background Information

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) called for the development of regulations to protect both the privacy and security of health information. This requirement was filled by the development of four rules, the Privacy Rule, the Security Rule, the Enforcement Rule and the Omnibus Rule, which together make up the national HIPAA compliance standard. The need for these rules arose from a lack of security standards, coupled with the widespread adoption of new technologies and a growing reliance on use of electronic information systems within the healthcare industry. The HIPAA rules are intended to protect patients' health information, while making it easier for healthcare organizations to adopt new technologies to improve efficiency of patient care. The Security and Privacy Rules make up the actionable items for healthcare professionals to follow; the Enforcement and Omnibus Rules pertain to upholding Security and Privacy and ensuring compliance.

What: HIPAA Security Rule, Privacy Rule, Enforcement Rule and Omnibus Rule; a national set of regulations to standardize the protection of confidentiality of patient medical records, otherwise known as PHI (protected health information).

Why: With no national security or privacy standards in place and a growing use of electronic systems in the healthcare industry, there was an increasing risk of patients' personal information being distributed without authorization or reason.

Who: The HIPAA Rules were developed by the Department of Health and Human Services (HHS). Within HHS, the Office for Civil Rights (OCR) is responsible for enforcing the Rules.The HIPAA compliance standards as determined by the Security and Privacy Rules apply to

> *"… health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA…"*

Validation cycle: Unlike other standards such as PCI DSS or SSAE-16 SOC2, there is no formally mandated audit or validation process (this is changing – see the Compliance section in the main body of this document). Fax service buyers are strongly encouraged to develop a detailed set of platform requirements based on the HIPAA standard. Simply asking if a vendor is HIPAA compliant is not enough.

HIPAA Compliance Requirements

1. Will your organization sign our HIPAA Business Associate Agreement? If not, please provide a copy of your standard BAA for review.
2. Has the organization completed a third party HIPAA compliance assessment? When was this last conducted? Please provide results.
3. Please provide contact information for your assigned HIPAA Compliance Officer and provide a brief summary of their experience.
4. Please describe the overarching process adopted by the organization to ensure compliance with HIPAA regulations.
5. Please describe how individual policies and procedures are maintained to ensure continuing compliance with changes in HIPAA regulations.
6. Please describe the HIPAA training employees receive.
7. Which teams/departments receive HIPAA training?
8. How often do teams/departments receive HIPAA training?
9. Who provides HIPAA training?
10. Are there regular security / privacy risk assessments conducted?
11. What is the process for reporting and responding to suspected or confirmed unauthorized disclosures?
12. Has the organization experienced an unauthorized disclosure in the last five years? If so, please provide details including timing, scope, cause, impact and remediation).
13. Please describe the platform/data center physical security provisions that specifically address the requirements for HIPAA compliance.
14. Please describe the platform's network security provisions that specifically address the requirements for HIPAA compliance.
15. Please describe the platform's logical and application security provisions that specifically address the requirements for HIPAA compliance.
16. Is there a HIPAA compliant records retention policy covering electronic faxes?

Appendix G - PCI DSS Compliance Requirements

PCI DSS Background Information

Formed in 2006 by the five major credit card companies (Visa, MasterCard, American Express, Discover and JCB), the PCI DSS is a standard for security protocol for any business, of any size, that accepts credit card transactions. This standard is applicable to any entity that handles, interacts with or stores payment card data. Adhering to PCI DSS involves a continuous process of assessing systems for vulnerability, remediating those vulnerabilities, and reporting compliance audits to the applicable payment card brands. PCI DSS standards are also used to guide the development and manufacturing of applications and devices used to conduct transactions, store or interact with payment info.

What: Payment Card Industry (PCI) Data Security Standard (DSS); a set of standards to combat vulnerabilities that may appear anywhere in the card-processing ecosystem, from transaction- and merchant-based activities, to systems operated by service providers.

Why: Vulnerabilities in the credit card transaction process have only grown with the advancement of the digital age and widespread adoption of web technology in everyday commerce. PCI DSS was developed to protect cardholder data and combat vulnerabilities in all types of transactions that involve use of a payment card.

Who: PCI DSS was established by the Payment Card Industry Security Standards Council (PCI SSC), an organization formed in 2006 by the five major credit card brands in the industry (Visa International, MasterCard, American Express, Discover, and JCB). The PCI DSS is an independent entity that both crafted and continues to oversee the PCI DSS to safeguard security throughout the entire transaction process. It should be noted, however, that merchants who accept credit card transactions are not accountable to the council; they are accountable directly to the relevant payment card company and the banks involved.

PCI DSS must be followed by any entity that accepts, transmits, or stores any payment information. For PCI DSS, there are two types of such entities: Merchants and service providers. A merchant is any entity that accepts Visa, American Express, MasterCard, JCB or Discover cards (one, some or all). A service provider is any entity (besides one of the five payment brands) that is directly involved in processing, transmitting or storing payment information, as well as any entity whose services might impact the security of the cardholder data. Concord Technologies and entities offering similar services are qualified as service providers. Some fax vendors may in fact need to be classified as both a Merchant and a Service Provider if they accept and process credit or debit cards for their services.

The PCI DSS Compliance Process: PCI DSS compliance isn't a one-time certification; it's a continuous process. The three ongoing steps for compliance are:

Assess: Identifying cardholder data, taking an inventory of your IT assets and business processes for payment card processing, and analyzing them for vulnerabilities that could expose cardholder data.

The primary goal of assessment is to identify all technology and process vulnerabilities posing a risk to the security of cardholder data that is transmitted, processed or stored. It It determines how cardholder data flows from beginning to end of the process – including PCs and laptops that access critical systems, storage mechanisms down to any printed materials where applicable.

Remediate: Fixing vulnerabilities and not storing cardholder data unless you need it. This includes technical flaws in software code or unsafe practices in how an organization processes or stores cardholder data.

Report: Compiling and submitting vulnerability scanning / penetration testing reports along with remediation validation records (if applicable), and submitting compliance reports to the acquiring bank and card brands you do business with.

Validation cycle: For service providers processing more than 300,000 accounts / transactions annually, a yearly on-site security audit is required. For service providers processing less than 300,000 accounts/transactions annually, an annual self-assessment questionnaire (SAQ) is required.

Both service provider types require a quarterly network scan and an annual penetration test.

PCI DSS Compliance Requirements

1. Is all of the specific infrastructure (primary and failover) used to provide the service proposed to clients covered under your PCI DSS compliance program?
2. Which PCI DSS Service Provider Level is the service classified as?
3. When did the organization first become PCI DSS compliant?
4. Have there been any periods in the last five years where the organization has not been PCI DSS compliant?
5. Has the organization experienced a data breach in the last five years? If so, please provide details including timing, scope, cause, impact and remediation.
6. Please describe relevant security measures used to ensure PCI compliant handling of regulated data. What measures are used to encrypt, redact and/or delete content?
7. Please describe how individual policies and procedures are maintained to ensure continuing compliance with changes in PCI regulations.

Documentation maintained by PCI DSS Level 1 Certified Service Providers:

1. COC Certificate of Compliance.
2. Annual onsite PCI data security assessment, completed by a Qualified Security Assessor (QSA).
3. Latest quarterly Network vulnerability scan performed by an external Approved Scanning Vendor (ASV).

Documentation maintained by PCI DSS Level 2 Certified Service Providers:

1. AOC Attestation of Compliance.
2. Self Assessment Questionnaire (SAQ) completed and signed by the dedicated Compliance Officer of the vendor organization.
3. Latest quarterly Network vulnerability scan performed by an external Approved Scanning Vendor (ASV).

Appendix H - SSAE-16 SOC2 Compliance Requirements

SSAE-16 SOC2 Background Information

System and Organization Controls 2, is one section of a comprehensive auditing suite that focuses on system-level controls of a service organization. Where SOC 1 focuses on the internal controls over financial reporting, SOC 2 concentrates on the protection and privacy of data.

What: The AICPA designed and established SOC 2 as the premier auditing standard to address the continuing trend of cloud computing. However, SOC 2 was not the original name, or even the original concept of this auditing standard.

The original standard, now known as SOC 2, was preceded by SAS 70, which provided guidance to the independent auditor to issue an appropriate opinion and report on the organization's control objectives.

In 2011, the Statement on Standards for Attestation Engagements (SSAE) No. 16 replaced SAS 70 and established a new attestation standard (AT 801). SSAE No. 16 later became SOC 1 to focus only on the financial controls. SOC 2 was developed to concentrate on data sent to service organizations, primarily to prevent misuse, whether intentionally or inadvertently.

Why: The growing presence of technology, cloud computing and SaaS service providers within the greater landscape of US service organizations has brought about the need for security standards for both proprietary data and personal information.

Who: SSAE 16 was created by the American Institute of Certified Public Accountants (AICPA). Each Service Organization Control (SOC) pertains to a different kind of organization; SOC 2 pertains to organizations offering services that are based in computer technology, SaaS or cloud computing.

Validation cycle: Annual audit required.

Documentation the fax service vendor should maintain:

1. SSAE-16 SOC2 Certificate for the organization providing the fax service.
2. SSAE-16 SOC2 Report for the organization providing the fax service.

Additional SSAE-16 SOC2 Requirements

1. Has the organization passed an SSAE-16 SOC 2 Type II audit in the last 365 days specifically pertaining to the services and /or products being proposed?
2. When did the organization complete its first SAE-16 SOC 2 Type II audit?
3. Have there been any periods since the above date where the organization has not been in possession of a valid SSAE-16 SOC 2 Type II audit report?
4. When is the next audit scheduled for?
5. Are any infrastructure components used to process fax traffic (in a primary, secondary or other capacity) excluded from the SSAE-16 SOC 2 Type II report or defined as “out-of- scope? If so, please describe.
6. Are any of your organization’s products, services, business units or departments excluded from the SSAE-16 SOC 2 Type II report or defined as “out-of-scope? If so, please describe.

Appendix I - FedRamp

FedRAMP Background Information

FedRAMP uses a standard to authorize cloud programs for use by a government agency within federal I.T. infrastructure. Then, details on that security authorization are stored in a repository so that other government agencies can use those details to leverage the same system within their own agency, without having to go through a full security assessment. The authorization details for a program are called an “authorization package” or “security package,” and the package info contains a comprehensive list of items that the program is used for, and thereby is authorized for. If a leveraging agency wants to utilize that program in any ways that aren’t included in the security package, they will need to undergo assessments specifically for those additional uses. Each individual government agency is responsible for doing ongoing assessments of the cloud service being used. The initial authorization makes a cloud service FedRAMP compliant, but FedRAMP is more than just the authorization; it’s the three-step process of authorizing, leveraging and assessing.

What: Federal Risk and Authorization Management Program; a government-wide program for standardizing security assessment, authorization and ongoing monitoring for cloud-based services/products that are being incorporated into Federal I.T. infrastructure.

Why: Each government agency has been responsible for managing its own security risks and providing security assessments and authorizations for each I.T. system it uses, even if other government agencies have already done so with the same system. Additionally, the current security assessment and authorization method used by the government fails to focus on maintaining visibility into real-time threats and how they’re mitigated. The combination of these two issues means that the use of cloud software within Federal I.T. is expensive, redundant in assessment/authorization processes and generally inefficient.

FedRAMP aims to counteract these issues by standardizing security controls to provide joint security assessments and authorizations; by using third parties to consistently evaluate a Cloud Service Provider’s ability to meet security controls; by enacting continuous monitoring services.

Who: FedRAMP was created primarily by government agencies, specifically “…cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.”

The FedRAMP Authorization Process

For each cloud system being utilized in the Federal I.T. infrastructure, a three-step process needs to be utilized.

Security assessment: Each prospective cloud service goes through an assessment process that uses one standard set of requirements, in accordance with the Federal Information Security Management Act (FISMA). Based on these requirements, a cloud system is either granted or denied security authorization.

Leveraging and Authorization: Federal agencies use the FedRAMP repository to view and leverage existing security authorization packages, then use that info to grant security authorization for the cloud system within their own agency.

Ongoing assessment and authorization: Authorized cloud systems must undergo ongoing assessment and authorization to maintain the security authorization.

Validation cycle: All FedRAMP authorizations must be renewed every three years.

There are three ways a cloud service provider can achieve FedRAMP compliance:

1. Attain a FedRAMP provisional authorization (P-ATO) through the Joint Authorization Board (JAB).
2. Work directly with agencies to obtain a FedRAMP agency authorization (ATO).
3. Work independently with an accredited 3PAO and supply a completed security package (without authorization) to the FedRAMP PMO.

References

https://www.hhs.gov/hipaa/for-professionals

http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate- agreement-provisions/index.html

https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20 Guide.pdf

https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC2Re port.aspx

https://www.fedramp.gov/resources/faqs/

About Concord

At Concord Technologies, our primary mission is to simplify the way that organizations interact with their crucial documents, with a focus on those organizations in compliance-oriented industries. For over twenty years, we've been enabling businesses to simply send, receive and manage their crucial documents using our secure, compliance-optimized cloud network. Today, we have over a hundred thousand users in the enterprise and healthcare industries who rely on Concord every day. For businesses in need of 24x7 on-demand, secure, compliant cloud fax and document management services, Concord provides a solution. We go above and beyond multiple standards of compliance, including HIPAA, SOC2 and PCI DSS compliance. Because of this, Concord's users consist largely of businesses that require a highly secure, available and compliant cloud fax network.