Maximising Fax Security; FAQ

Q: Why should security be a priority for digital transformation initiatives today?

A: When it comes to security, much is made of how existing systems are ill suited to tackle modern threats. Many organisations are in various stages of their digital transformation journeys, and as they each digitise their operations, they also increase their risks, but their security processes have yet to evolve at the same rate.

Q: How are digital transformation and security relevant to the fax?

A: The fax is a critical communications device. Nearly 17 billion faxes are sent around the world every year, while in the UK, more than 125,000 were sent and received by the public sector in 2019. In the US, it accounts for 75% of medical communication.[1]

In 2018 the traditional fax machine technology was dismissed as "archaic" by health secretary Matt Hancock,[2] with the Minister for Health and Social Care mistakenly declaring that "everyone else got rid of them years ago". He went on to name check email as being more secure and effective, and set a deadline for the removal of all fax machines from the NHS.

Simply banning fax is not an option without an appropriate alternative secure solution, while the suggestion that email is a like-for-like replacement is undermined by the fact that if that were the case, the sectors that rely on fax for certain communication would have migrated over a long time ago. Ultimately, there are too many businesses and vital services that rely on the fax on a daily basis to dismiss it as a relic that needs replacing, without considering how.

Q: Why isn't traditional analogue faxing a secure option?

A: For the majority of organisations, this simply is not practical. Digitalisation is driving ever greater levels of efficiency, cost savings, operational optimisation, and innovation – inserting any sort of analogue technology could diminish those benefits.

In the case of faxes, while the traditional telephone line is not digital, and therefore not hackable, faxes are not encrypted in transit, so anyone with access to the line can, theoretically, also have access to the information sent via a traditional fax machine. The fact that it is unencrypted runs counter to many governance, compliance, and industry-specific regulatory concerns.

Q: Is human usage the real security threat to the fax?

A: Traditional paper based fax machine location and output is a security issue for all organisations.

Often in the centre of open plan offices, or certainly not in a secure office, and left unmonitored for the majority of the time, a sensitive fax could sit out in the open for some time until the recipient collects it. That is before one considers how often physical documents have been misplaced, stolen, or exposed.

These all link back to the human factor in data breaches – where mistakes by people are the number one cause. It's no different for faxes. While all forms of communication are prone to human error, faxing has to contend with the sheer number of mistakes that can easily be made when dialling a phone number.

Q: Is there a secure alternative for organisations who rely on the fax?

A: The answer lies in one of the technologies driving digital transformation – cloud computing. With no upfront costs and no physical hardware, the cloud provides easy access to the technology a business needs.

Digital cloud faxing does exactly this, but for faxes. It allows the entire fax process to be handled digitally via the cloud; either through a company's email application, an MFD, workflow application, mobile app or secure web-portal.

Users no longer have to rely on a physical fax machine at either end. If party A requires an order via fax, party B can now simply use a digital cloud faxing app to upload and share the required information.

Q: How secure is digital cloud fax?

A: digital cloud fax does more than improve flexibility – it dramatically increases security. Cloud faxing provides high-level encryption, both in transit and when faxes are stored, as well as audit trails of everything sent and received, improving governance and compliance where required.

On top of this, administrators can implement access restrictions, just as they would with any other data. With digital cloud faxing, security professionals can implement the same cyber hygiene principles to faxing that they apply across the organisation – from access management, to implementing passwords and password behaviour, and the ability to update the software being used automatically.

By integrating digital cloud fax into their digital transformation initiatives, enterprises can ensure that they have consistent levels of security across all their communications channels.

Q: How can eFax help organisations become more secure?

A: Traditional fax equipment can place enterprises at a security risk. There is also a risk of non-compliance with industry regulations, including GDPR. Processes have to meet industry standards for protecting data.

eFax has been a leader in fax compliant solutions for more than 25 years. We help ensure that faxes are transmitted securely and accessible only to authorised personnel — helping organisations in a wide variety of sectors meet confidentiality requirements.

Our eFax Secure™ solution protects and secures sensitive and confidential faxes, offering an email-driven and convenient process for receiving faxes securely over the web, while remaining compliant with a variety of data regulations, from the Data Protection Act to GDPR.

Q: Provide an example of how you have helped an organisation securely transform their fax communications?

A: Moorfields Private is the private division of the Moorfields Eye Hospital NHS Foundation Trust. It's the leading provider of eye health services in the UK and a world-class centre of excellence for ophthalmic research and education.

Security was at the top of its lists of priorities, with a requirement for fax transmission encryption, fax data retention and archiving, centralised control of the faxing function, and the ability to provide secure fax access to select hospital and administrative staff.

Sensitive documents no longer sit openly on a fax machine and staff can be more productive as they no longer need to wait by a fax machine. And because faxes are now in digital format, administrative staff can retrieve and access patient records much quicker and respond to queries in a shorter timeframe, improving patient services.

Q: What are the security standards for digital cloud faxing?

A: Whether an NHS trust, government department or private sector enterprise, you need to know that your cloud fax provider has the highest levels of security and compliance for your communications.

As standard, they should offer:

- Highest Encryption Levels to ensure data is protected as it travels from point to point: 256-bit AES and TLS encryption protect your inbound faxes immediately.
- Tier-III Secure Servers: Servers in highly secure data centres keep your faxes protected 24/7/365.
- Transport Layer Security (TLS) to create a trusted, secure link from point to point: Secure channel open and a PIN required when you access your fax online.

Technology specific security questions

Q: We understand that eFax can integrate with Active Directory via LDAP – do you support secure LDAPS to ensure that any sync between eFax and PMC is secured?

A: At this time, we do not offer an Active Directory sync connector, although an integration with Active Directory is achievable via further customer development. Currently, all API calls are secured using TLS technology over an HTTPS session and the API call authentication process uses the same credentials used to log into the eFax Admin Portal.

Can you confirm the following for the web browser service:

Q: Does the solution support a unique username for each user of the solution for audit purposes?

A: Our product supports using unique usernames/ passwords, which can be used for logging and audit trail purposes. There are two areas where this method is implemented: For users, the email or eFax number and their password are required. For Administrator a five-digit account code, password and Administrator Name are required.

Q: Is authentication information such as passwords hashed when at rest?

A: Yes, passwords are hashed and encrypted using 256-bit AES encryption for added layer of security. Furthermore, we follow all the security rules for HITRUST CSF Certification in the USA, which is the highest standard for security compliance for healthcare.

Q: Does the solution support an account lockout policy in case of multiple login failures?

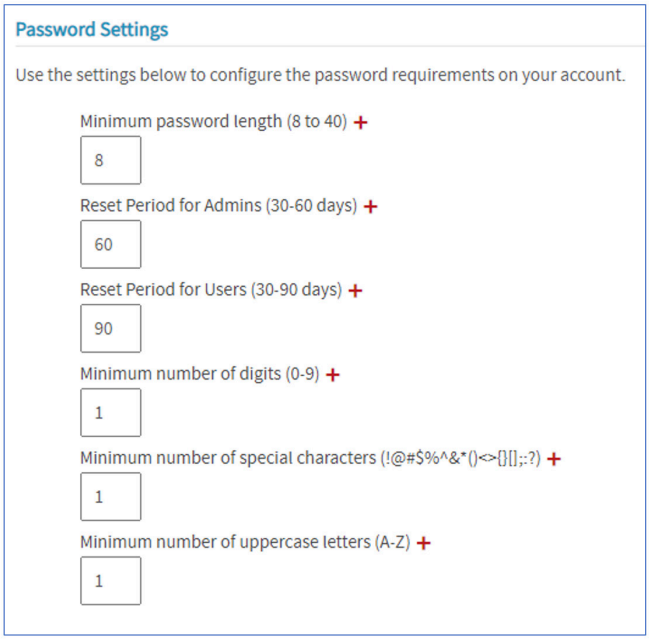
A: Yes, after 5 attempts the account is locked for security purposes.

Q: Does the solution support strong password policy (e.g., password minimum length, complexity of password, password change every X days etc.)?

A: Yes, we support strong passwords. The password requirements are provided in our web portals, user guides, and API documentation.

Q: What strong password options are provided? Can these options be set centrally to apply to all users?

A: Yes, the default settings and requirements are in the following screenshot.



Q: In the event that a fax is sent via the web browser, is any data stored on eFax servers relating to the content of that fax?

A: No, there is no data stored on eFax servers related to the content of any electronic faxes. Faxes and electronic faxes are inherently pictures of documents. A fax can contain graphics and text, but that content is not captured – or tracked – by eFax.

Our product can, in some cases, store the fax image. But this would only occur if the customer has requested that Send Storage feature is enabled on their account. This setting is disabled for all new accounts by default and only available upon request.

Q: In the event that data is stored, can automatic data retention policy be applied e.g., any stored faxes be deleted after 90 days etc?

A: The product does not store Send (i.e. sent) faxes; eFax is a 'pass-through' technology. For Inbound (i.e. received) faxes, a storage retention period can be set in days if a customer requests it.

Q: Does eFax intercept and protect against malware being sent on the eFax service?

A: Yes, our product has numerous security measures in place, with regular, periodic reviews, and process and software updates to guard against any threats from spam, malware and other fraudulent activity.

Q: How is the user notified if a fax sent on the eFax service contains malware and is intercepted by eFax?

A: When this occurs, eFax blocks the Outbound/Send fax email message and does not allow it onto our network. What we receive is a TIFF/Analog document for Inbound/Received faxes without any further attachments.

Q: Can you confirm where the eFax notifications service for new releases/security advisories is located so subscriptions can be setup?

A: Confirmations will be emailed to the email address associated with the User Profile. The eFax team makes every effort to notify all our customers of product updates, outages, and security issues via email.

Q: This requirement relates to eFax security advisories – does eFax provide a subscription service to notify PMC of security incidents, new releases of the eFax service etc?

A: As part of the contract the Administrator would receive notification from our Customer Support group. Furthermore, the eFax team makes every effort to notify all our customers of product updates, outages, and security issues via email.

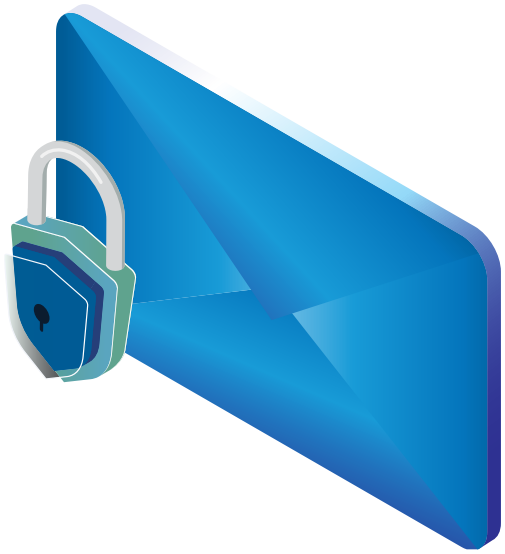
Q: Can you provide an example of a recent security advisory announcement or new release notification sent out by eFax?

A: Product announcements can be seen on our website/news section. For example, when a major product milestone was reached, we announced the HITRUST Certification (link: https://enterprise.efax.com/news/2019/10/30/j2-global-inc.-achieves-hitrust-csf-certification-to-mitigate-further-risk-in-third-party-privacy-security-and-compliance). Our team also provides useful security notifications and we have an Incident Response Plan to deal with any breaches, along with notifications.

Q: What is the HITRUST Common Security Framework (CSF) certification.

A: In the USA's healthcare industry, a HITRUST CSF certification acknowledges that eFax utilizes a well developed and well recognised framework for regulatory compliance and risk management. The framework is developed in collaboration with information security professionals. It incorporates nationally and internationally accepted standards, including ISO, NIST, PCI, HIGHTECH and HIPAA, to ensure that certified organisations maintain a comprehensive set of security controls.

The HITRUST CSF certification is considered by many to be the "gold standard" for a compliance framework in the healthcare information industry. It is the most comprehensive and most widely applied security framework in the U.S. healthcare system. According to HITRUST, 81 percent of US hospitals and 80 percent of health plans have adopted the framework in some way. eFax is proud to become the first major cloud fax provider to achieve this certification.



Q: Why is the HITRUST Common Security Framework (CSF) certification important?

A: Achieving the HITRUST CSF certification is a notable accomplishment. It reflects the highest level of commitment to security and compliance in an organization.

Effectively managing data, information risk and compliance is complex in today's ever-changing digital landscape. There are many components and considerations in developing and implementing a program that encompasses and integrates all the elements needed to manage this risk and maintain compliance.

Obtaining CSF certification is a rigorous assessment process that demonstrates an organisation's commitment to that objective. It involves multiple stages of self-assessment, CSF assessment and review, and a HITRUST quality assurance review.

By obtaining the HITRUST CSF certification, organisations are following a framework that is constantly evolving and upgrading to reflect the latest changes in the industry. Certificate holders also avail themselves to a broader approach that includes proactive threat anticipation, assessment and corrective action plan management, automated assurance sharing, a scalable and transparent means of providing security assurances to stakeholders, and a third-party risk management process.

Q: Why should customers care (HITRUST CSF Certification)?

A: Some of our present and future customers may ask why this is important. What, if anything, will you get out of this certification? It is a fair question, and one we are more than happy to answer.

As an eFax customer, you entrust us to deliver state-of-the-art cloud fax technology to help you meet your own customers' needs. They are entrusting you with their most sensitive and confidential personal health information, and you are entrusting us with that same information.

eFax has always maintained the highest standards of privacy, security and regulatory compliance. We incorporate a number of safeguards. Our digital cloud fax technology (DCFT) is designed to comply with financial security and privacy regulations, including HIPAA and GLBA. It meets the most stringent requirements for secure document transmission, in compliance with the recommendations of the National Institute of Standards and Technology (NIST). We protect data at rest according to the Advanced Data Encryption (AES) standard. Your fax data resides in eFax's Tier III/IV-rated, highly secure colocations and private data centres. We keep your data stored redundantly. Finally, two-factor authentication (2FA) adds a second level of authentication.

All of the above ensures that your data receives maximum protection. By undergoing the process to achieve the HITRUST CSF Certification, and by earning that certification, eFax has further demonstrated its commitment to maintaining the highest standards in the industry, and we have added another layer of assurance to our customers. And all of this is at no cost to you.

Quality Management System Compliance

Q: Do you have a documented quality management system? For example, is your system compliant with a recognised quality management standard, such as ISO 9001.

A: eFax is compliant with ISO 27001 controls, which is more aligned to services like our cloud fax technology, and this is included in our existing HITRUST CSF certification.
eFax complies with following recognised certifications and standards:

- HITRUST (certified)
- SOX (certified)
- PCI-DSS (certified)
- HIPAA / HITECH ACT
- GLBA / FFIEC (financial)
- ISO 27002 STANDARDS (27001 is the certification process)
- SAS70 / SSAE16
- GAPP (generally accepted privacy principles)
- iGRC – (integrated governance, risk, and compliance)
- GPG-13 (good practice guide 13, UK standards)
- SOCO (framework)
- COBIT (framework)
- OWASP (framework)
- SDLC (framework)
- SECURITIES AND EXCHANGE COMMISSION
- CFR TITLE 21 (FDA DEPENDANT)
- GCP PART 11 (FDA DEPENDANT)
- MASSACHUSETS PRIVACY LAW 201 CMR 17
- EU DATA PROTECTION DIRECTIVE
- NISPOM (standards – DoD)
- SANS CRITICAL SECURITY CONTROLS (standards)

Q: If your quality management system is not certified under ISO 9001 (or similar), how do you ensure the quality of the products or services to be provided?

A: eFax and its cloud services are ISO 27001 certified and this is factored into our HITRUST CSF certification process. The team is often asked about ISO 9001, but this is more appropriate for manufacturers of hard goods, which are different to our cloud software services. In addition to ISO 27001 certification, our faxes are processed through TIER III/IV colocations that are SOCII compliant; this means that our company follows a rigorous audit process to ensure customer data is securely managed and privacy is protected. This includes ensuring faxes are encrypted at rest and during transmission.

Q: What is the process adopted to verify and vet staff who, it is anticipated, will attend or have access to our premises, information systems or information assets?

A: Our company has well-established processes for vetting staff who are anticipated to have access to sensitive information. Our Human Resources team performs background checks on this staff, including employment history, education, and credit. We also place process safeguards to ensure only the appropriate team members have access to sensitive data.

Q: Do your employment contracts with staff and contracts for the appointment of sub-contractors and/or agency workers include confidentiality clauses?

A: Yes, contractors adhere to same conditions as employees.

Q: Do you train your staff on the care and secure handling of personal data and information security?

A: Yes, we provide annual training on PCI, PII, computer safety, phishing, malware and email safety. All employee training is handled by InfoSec and results are handled by HR.

Q: What records do you maintain to record which of your staff accesses client premises or information and when that access occurs?

A: eFax logs what account and transactions are accessed by employees or we can see by the IP address what customers have accessed.

Q: Are eFax user data transiting networks adequately protected against tampering and eavesdropping?

A: Yes, our services offer secure connectivity via TLS v1.2, an industry standard to protect data in transit. For Outbound (e.g. sending faxes) we offer an optional service to enforce secure connectivity using TLSv1.2, by instructing the users to send faxes using the domain @efaxsendsecure.eu. Examples of this usage can be found in our product guides and quick start guides.

Q: Is user data, and the assets storing or processing it, protected against physical tampering, loss, damage or seizure?

A: All fax images and user account information are encrypted using AES 256-bit encryption and stored within Tier III or IV data center facitilies. These are industry-leading tiers for security and maintenance.

Q: Is a malicious or compromised user of the service able to affect the service or data of another?

A: With all eFax services there is a logical separation between users.

Q: Do you have a security governance framework that coordinates and directs management of the service and information within it?

A: eFax has been reviewed and tested against the following frameworks and standards:

- SOX (certified)
- PCI-DSS (certified)
- HIPAA / HITECH ACT
- GLBA / FFIEC (financial)
- ISO 27002 STANDARDS (27001 is the certification process)
- SAS70 / SSAE16
- NIST/FISMA - E-GOVERNMENT ACT, TITLE III
- GAPP (generally accepted privacy principles)
- iGRC – (integrated governance, risk, and compliance)
- GPG-13 (good practice guide 13, UK standards)
- SOCO (framework)
- COBIT (framework)
- OWASP (framework)
- SDLC (framework)
- SECURITIES AND EXCHANGE COMMISSION
- CFR TITLE 21 (FDA DEPENDANT)
- GCP PART 11 (FDA DEPENDANT)
- MASSACHUSETS PRIVACY LAW 201 CMR 17
- EU DATA PROTECTION DIRECTIVE
- NISPOM (standards – DoD)
- SANS CRITICAL SECURITY CONTROLS (standards)

eFax also maintains a strong governance of compliance, including our Security Policy as well as other written procedures that take into account many security and compliance frameworks. We also comply with the requirements of the HITRUST CSF framework and the PCI-DSS requirements for Merchants and Service Providers.

Q: Does eFax operate a security policy?

A: Yes, we can provide further information upon request.

Q: What is included in the eFax security policy?

A: Our security policy outlines how the eFax service is operated and managed securely in order to impede, detect or prevent attacks.

The document also includes our security policies on:

- **Personnel security:** Where personnel may have access to your data and systems, clients need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise.

- **Secure development:** Where services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise data, cause loss of service or enable other malicious activity.

- **Supply chain security:** This ensures that our supply chain satisfactorily supports all of the security principles which our service claims to implement.

- **Secure user management:** This ensures we make the tools available for clients to securely manage their use of our service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of client resources, applications and data.

- **Identity and authentication:** This ensures access to service interfaces should be constrained to authenticated and authorised individuals.

- **External interface protection:** This is where all external or less trusted interfaces of the service should be identified and appropriately defended.

- **Secure service administration:** Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

- **Audit information for users:** The provision of audit records needed to monitor access to the eFax service and the data held within it. The type of audit information available to eFax will have a direct impact on our ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

- **Secure use of the service:** The security of cloud services and the data held within them can be undermined if the service is used poorly. Consequently, eFax has certain responsibilities when using the service in order for client data to be adequately protected.

Health & Safety

Q: Who is responsible for Health & Safety?

A: Our Network VP and Chief Information Security Officer (CISO).

Q: What are their Health & Safety qualifications and position?

A: Their qualifications include a Master of Science degree in AI, Computer Science, Agile Methodologies, HIPAA, CTO, CISSP, CISA and ITIL.

Q: Have any formal notices or legal proceedings been taken against your organisation by the Health and Safety Executive in the last 3 years?

A: No.

Q: How often are your Health and Safety management arrangements reviewed?

A: Our company holds a regular internal audit every year and it is performed by a 3rd party.

Q: How do you consult with your employees on matters for Health and Safety?

A: Our company provides regular training on various compliance and security subjects for all our employees.

[1] https://www.vox.com/health-care/2017/10/30/16228054/american-medical-system-fax-machines-why
[2] https://www.gov.uk/government/news/health-and-social-care-secretary-bans-fax-machines-in-nhs

About eFax

eFax launched its digital cloud fax service with the goal of using the convenience of email and the speed of the internet to make it easier for people to send and receive faxes. eFax lets users and our 11 million customers receive, review, edit, sign, send and store faxes by email or through a web interface. Our appeal and success are built around three key features: the widest selection of phone numbers; an easy way to send and receive faxes and voicemail by email; and a fast, reliable and secure communications network.

To learn more about outsourcing to a digital cloud fax model with eFax, visit us at: eFaxCorporate.com

European Headquarters

eFax
European Headquarters
Unit 3, Woodford Business Park
Santry, Dublin 17, Ireland

Contact Sales:
UK 0800 689 0588
Rest of Europe +353 (1) 656 4950

Web:
eFaxCorporate.com

Follow Us

Please Recycle