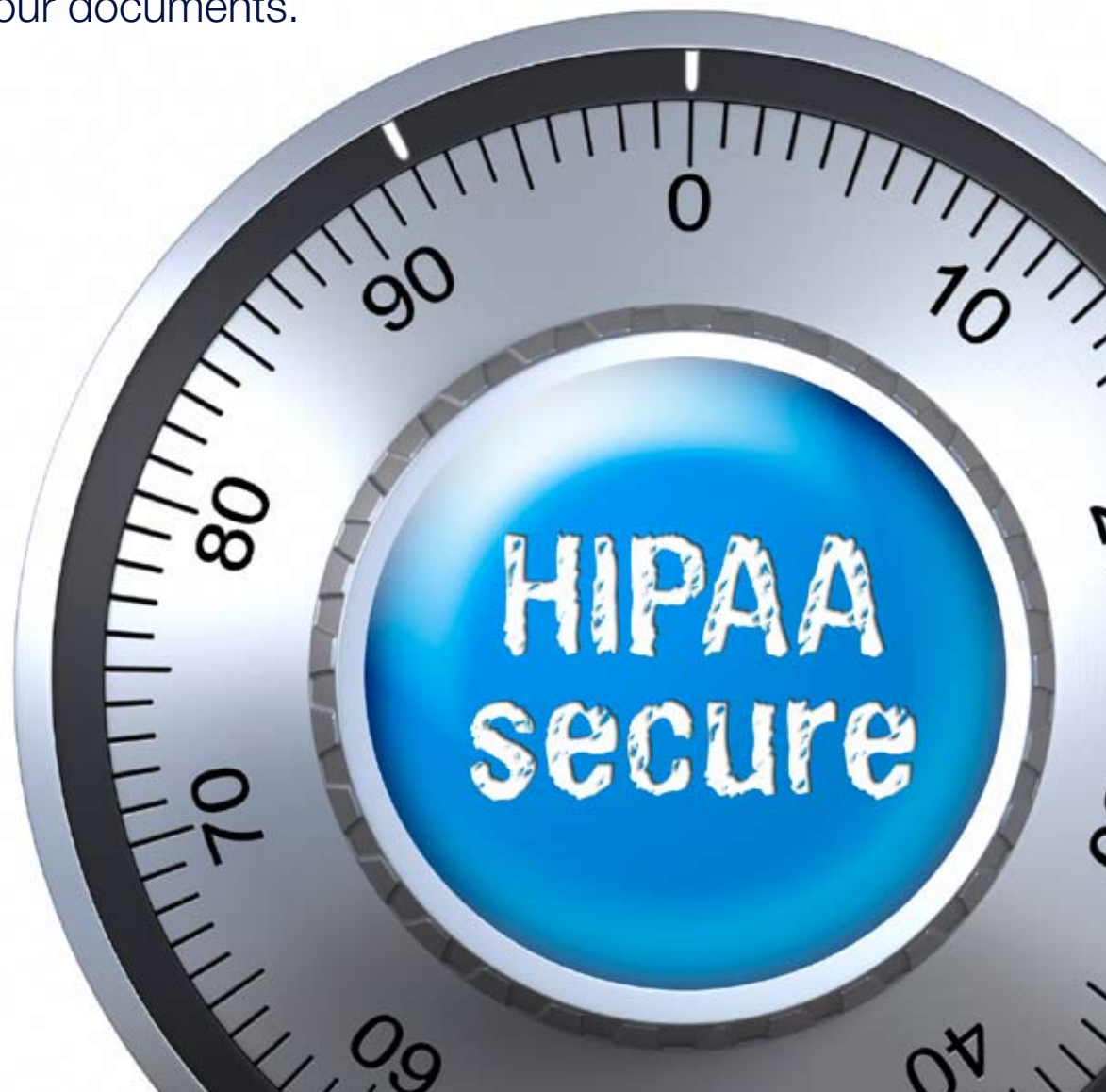


## So, why is Sfax HIPAA secure?

In today's connected world of healthcare, you're right to be concerned about document security and HIPAA compliance.

Uncover the reasons why Sfax is the safest faxing choice for your documents.



SecureCare's Sfax is a cloud-based fax solutions intrinsically superior to manual faxing, and are entirely capable of meeting the specific HIPAA requirements for faxing.

## Introduction

The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) establishes regulations for the use and disclosure of an individual's Protected Health Information (PHI) held by 'covered entities' (typically clearing houses, employer-sponsored health plans, health insurers and medical service providers).

Such 'covered entities' can send/receive PHI through Sfax cloud-based fax services entirely confident that Sfax can help them meet the HIPAA requirements for faxing.

SecureCare may be defined as 'Business Associate' (BA). A BA is a person or organization that performs certain services for a covered entity, involving the use and/or disclosure of PHI. When PHI is faxed from a computer, HIPAA security measures need to be implemented by the covered entity and BA.

According to the Security Standard Final Rule, a covered entity may permit a BA to create, receive, maintain or transmit ePHI on the covered entities behalf only if the BA obtains satisfactory assurances, in accordance with §164.305(a) that the BA will appropriately safeguard the information. This document is intended to provide assurance that SecureCare will safeguard all information faxed to and from covered entities while using the Sfax service. SecureCare have implemented physical, organizational and technical safeguards necessary to protect the confidentiality and integrity of the information being communicated using Sfax.

## HIPAA & Faxing Requirements

HIPAA has particular requirements for faxing PHI to ensure that the privacy and security of the information is protected throughout the entire document lifecycle.

Not only are Sfax's cloud-based fax solutions intrinsically superior to manual faxing, and are entirely capable of meeting the specific HIPAA requirements for faxing:

- Incoming faxes do not sit on publically-available fax machines. They are automatically routed to a recipients secure inbox.
- Senders select recipients from established lists reducing the chance of incorrectly specifying the destination fax number.
- Notifications are sent to recipients inbox with link to specific fax.
- Cover pages are tightly controlled.
- Complete end-to-end audit trail of all fax activity.

A circular stamp with a light blue background and a white border. The words 'HIPAA' and 'secure' are written in a white, hand-drawn, chalk-like font, stacked vertically in the center of the stamp.

SecureCare has plethora of physical, organizational and the technical measures to protect the confidentiality and integrity of information being communicated using its Sfax services. Our safeguards combined with our smart faxing technology means that Sfax delivers the highest levels of security in the automated processing, exchange and management of sensitive documents and data.

## Our Data Centers

SecureCare's fax production equipment is located at facilities that provide 24-hour physical security, redundant electrical generators, redundant data center air conditioners, and other backup equipment designed to keep servers secure and continually up and running.

- **Perimeter Defense.** The network perimeter is protected by multiple firewalls and monitored by intrusion detection systems — all sourced from industry-leading security vendors. In addition, SecureCare monitors and analyzes firewall logs to proactively identify security threats.
- **Internal Systems Security.** Inside of the perimeter of firewalls, systems are safeguarded by network address translation, port redirection, IP masquerading, non-routable IP addressing schemes, and more.
- **Server Management Security.** All data that is provided by a customer is owned by that customer. SecureCare employees do not have direct access to the SecureCare production equipment, except where necessary for system management, maintenance, monitoring, and backups. SecureCare does not utilize any managed service providers. The SecureCare Operations team provides all system management, maintenance, monitoring, and backups.
- **Reliability and Backup.** All networking components, SSL accelerators, load balancers, Web servers, and application servers are configured in a redundant configuration. All customer data is stored on a primary database server that is clustered with a backup

database server for redundancy. All customer data is stored on disk storage that is mirrored across different storage cabinets and controllers. All customer data is automatically backed up to another disk array on a nightly basis which in itself is backed up to an external device. Disaster recovery plans are in place.

## Our People & Policies

The information contained in faxed documents is proprietary to the customer sending the fax. SecureCare employees do not have access to the SecureCare production equipment, except where necessary for system management, maintenance, monitoring, and backups.

The SecureCare servers that process faxes are housed in a secure environment that is accessed by a team of approved professional engineers and security specialists only. As a result, all information passing through SecureCare' internal server environment remains protected and secure.

We utilize the latest smart technology to provide the highest security levels to exceed the rigors of HIPAA compliance.

## Our Technology

- **Data Encryption.** SecureCare leverages the strongest encryption products to protect “customer data and communications, including 128-bit SSL Certification and 1024-bit private keys. The lock icon in your internet browser indicates that data is fully shielded from access while in transit.
- **User Authentication.** Users can access the Sfax service via printer driver or online only with a valid username and password combination, which is encrypted via SSL while in transmission.
- **Application Security.** Our robust application security model prevents one SecureCare customer from accessing another’s data. This model is reapplied with every request and enforced for the entire duration of a user session.
- **Operating System Security.** SecureCare enforces tight operating system-level security by using a minimal number of access points to all production servers. We protect all operating system accounts with passwords, and production servers do not share a master password database. All operating systems are maintained at each vendor’s recommended patch levels for security and are hardened by disabling and/or removing any unnecessary users, protocols, and processes.
- **Database Security.** Database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a number of points, and production databases do not share a master password database.

# UNDERSTANDING FAXING & SFAX.



With its ease of use, immediacy of delivery and universal accessibility, fax will remain a worldwide business standard for years to come.

## Secure Faxing

Manual faxing using today's standard PSTN-based fax transmissions is inherently secure, because hacking into a PSTN line requires physical access to the line or switching equipment. Cloud faxing with Sfax is even more secure because of the way the fax is transmitted. A hacker can't intercept a fax and even if they did it would appear as nothing but noise. That's because a fax is disassembled and converted into base64 binary, and then reassembled on the other end either within a fax machine or to an electronic fax service that decodes the binary image files. And with Sfax it gets even better because we add a layer of 128-bit encryption around everything.

## Technical Stuff

The reason faxing is seamless because modern fax machines operate using the same protocol, namely the Group 3 Facsimile protocol (G3). The G3 protocol was first published in 1980 by the ITU-T (International Telecommunication Union). The G3 standard for facsimile communications over analog telephone lines was originally approved by the CCITT in its T.4 and T.30 recommendations in 1980. This standard is supported by nearly every fax machines in use today and continues to be updated.

G3 is specified in two standards, T.4 (image-transfer protocol) and T.30 (specifies the session-management procedures that support the establishment of a fax transmission). Since G3 is specified for switched analog

networks, and it is an all-digital procedure, it must use modems or a fax relay. Real-time IP fax transport is specified in the new T.38 protocol and replaces modems. T.38 is an IP-based protocol that closely inter-works with T.30 to enable the same fax procedures over IP in real-time. T.38 only passes images, not files that could potentially contain viruses, worms, or Trojans. T.38 also only handles image data that is not executable. Sfax uses special hardware that transmits information only via the T.30 and T.38 "fax only" protocols.

In simple terms, T.30 is a fax handshake protocol that describes the overall procedure for establishing and managing communication between two fax devices - agree on such things such as transmission speed and page size. Because T.30 does not allow for the processing of data or the transmission of data, and only allows for the transfer of fax images in base64 binary (known as T.4 and T.6 images), there is no way to pass data through the fax service, either for removing data from the network or uploading malicious code.

Our 'fax only' hardware interprets the content of the data that was sent to it, either over the PSTN or over the IP network, prior to passing it on to the network. This interpretation means that malicious code cannot pass through. If the data is not a valid T.30 message, it gets dropped. If anything other than image information is embedded in the image data, the error handling that is implemented during image decoding discards it.

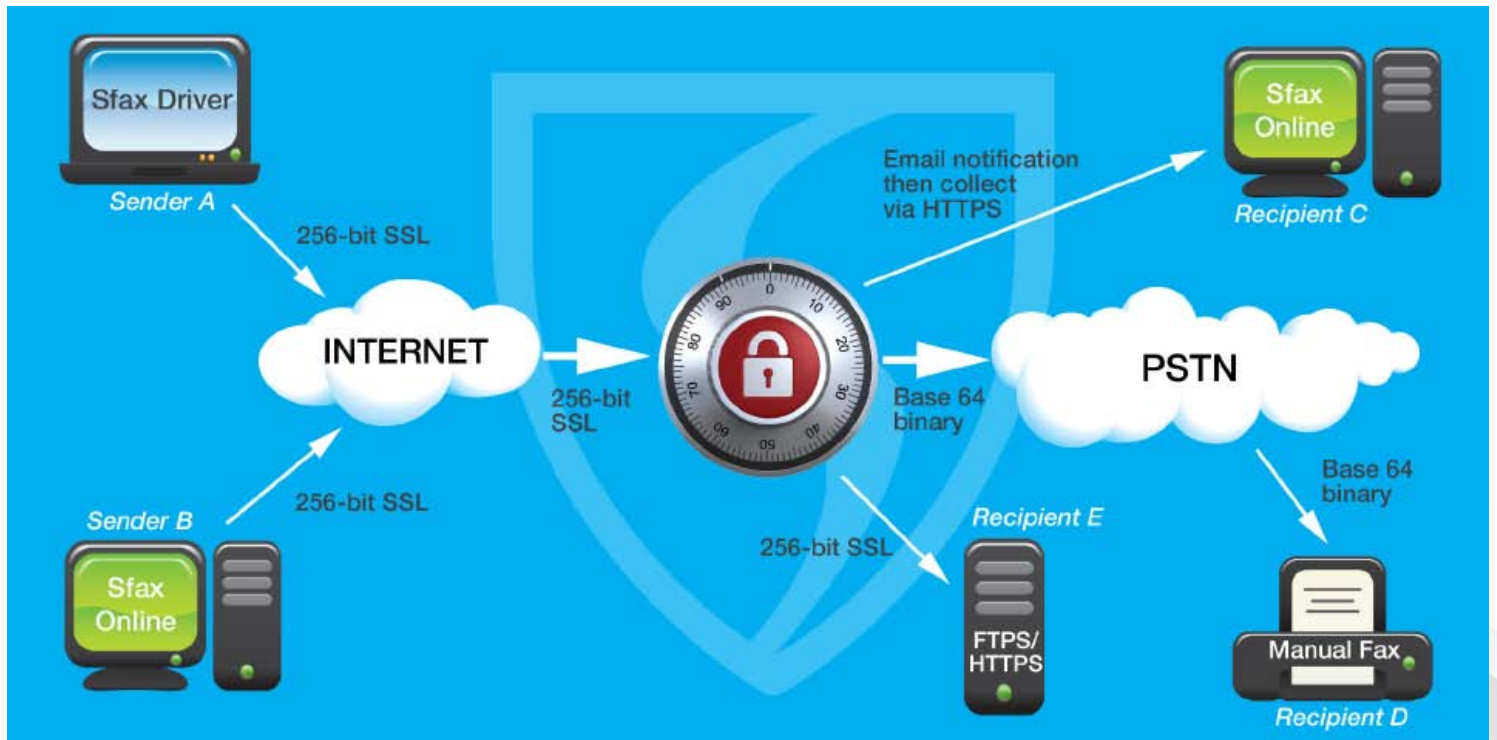


Figure 1 - Schematic diagram of Sfax security.

## Avoid Fax-to-Email and Email-to-Fax Services

Unlike the plethora of other fax-to-email providers, Sfax does not use email to transport documents at any point in the process. Although email is used every day, it is inherently insecure and is much like sending a postcard. Unfortunately, businesses transport PHI by email every day because they misunderstand or dismiss the risks.

When you use a fax over email service, that email content and any documents attached get read and stored multiple times en route by ISPs, servers, firewalls, virus checkers and unscrupulous 'bots' that harvest email data and the content within attachments. We only use email for notifications and not natively for the exchange of documents. The other issue with fax over email is that it is difficult to track missing faxes. With Sfax, we provide a complete audit trail with the ability to

track the document exchange through the entire lifecycle with industry-leading delivery rates and exceptional error reporting and handling.

## Fax Delivery

We only send email notifications by email that simply have a link that forces an individual receiving the fax to login to our server and retrieve the faxes from our HTTPS web application. We can also deliver faxes via FTPS (FTP over SSL) or HTTPS. FTPS creates a fully secure tunnel between the user and our servers. Our patent-pending Sfax Printer Driver can connect through the internet on a port that we secure and communicate on that port from the local user to our servers in our data centers.

Sfax does not store any personal information. The only information we utilize is the user's name, email address, username and password to establish an account.

# NEED TO KNOW MORE?



We have more healthcare experience than any other cloud-based fax provider. Get in touch so we can alleviate any remaining concerns and start building a relationship.

## Talk to Us

If you have an specific security questions, then speak to our compliance team who will advise how Sfax can help you meet the rigors of HIPAA.

SecureCare Technologies, Inc.  
4611 Bee Caves Road, Suite 306  
Austin, TX 78746

Tel: **888.447.3707**  
Sfax: **866.734.7706**  
Email: [sales@sfaxme.com](mailto:sales@sfaxme.com)  
[www.sfaxme.com](http://www.sfaxme.com)

## About SecureCare

SecureCare Technologies, Inc. has spent 10 years harnessing smart messaging and document exchange solutions to help organizations eliminate paper and improve business processes.

SecureCare started out designing HIPAA-compliant solutions for the healthcare sector. SecureCare's products are now loved by thousands of customers every day in a multitude of sectors including financial services, healthcare, insurance, legal, logistics, manufacturing and retail exceeding the compliance requirements for Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX) and Gramm-Leach-Bliley (GLBA).

A large, light blue circular graphic with a white border, containing the text 'HIPAA secure' in a white, hand-drawn style font. The graphic is set against a background of a large, faint clock face with numbers 70, 80, and 90 visible.

HIPAA  
secure