HIPAA Compliance for Faxing Services

Retarus Fax Services For HIPAA compliance and protection of electronic health information for healthcare service providers

What is HIPAA?

The Health Insurance Portability and Accountability (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) acts, enforced by the U.S. Department of Health and Human Services, provide federal protections for personal health information and give patients an array of rights with respect to that information. U.S. law mandates the guidelines for collecting, storing, transferring, and managing a patient's health records, and includes defining the BAA and PHI requirements that organizations are required to comply with. The law further specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information (ePHI).

The Impact of Non-Compliant Faxing on Organizations:

The Privacy Rule allows covered health care providers to share protected health information without patient authorization, as long as they use reasonable safeguards when doing so. These communications may occur orally or in writing, by phone, fax, e-mail, or otherwise. Despite being a legacy technology, fax is still the dominant way to communicate patient health information. According to a 2012 National Physicians survey, 63% of healthcare providers believe fax will continue to stay for decades. As fax is an extension of paper and as fax providers continue to integrate with various network, email system, mainframe, ERP, CRM, or ECM system, Health IT EMR/EHR, and ePrescription systems in the health IT industry, fax remains the interoperability standard for healthcare.

Faxing, however, still presents challenges to organizations dealing with HIPAA compliance including securing sensitive personal data managed within enterprise information infrastructures. As organizations scale, it become more critical to build additional infrastructure to support increased communication volume. As the fax machines and fax servers pile up in an organization, it leads to multiple points of failure and increased risk of security breaches as well as sky rocketing costs. For example, hard-copy documents left on fax printers can result in unauthorized access to personal information, resulting in breach of handling confidential data with costly penalties, litigations and damage to business relationships and corporate image. The penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision. Violations can also carry criminal charges that can result in jail time. As the risks are increased in these types of organizations, it leaves many within healthcare to consider a better, less costly, and more secure solution to traditional faxing.

Violation	Amount per violation	Violations of an identical provision in a calendar year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect — Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect — Not Corrected	$50,000	$1,500,000

Source: HHS, Federal Register.gov

HIPAA Compliance for Faxing Services

retarus: global messaging

What's required in a Cloud Solution?

- **Security**

HIPAA mandates that all patient information must be stored in secure facilities, with physical access limited to those personnel who are authorized to handle the data. Inherent with security is protecting and securing where faxes are received as well as securing where and how faxes enter the network. Ensuring both the proper physical and technological protocols are in place represents significant operational control challenges to any organization, including providing both critical aspects of a time-efficient and fully compliant solution. For cloud providers, they must be able to guarantee that its infrastructure is protected from the threat of unsanctioned access, as well as ensuring that the data at rest and in-transit are completely secured at all times.

- **Access control**

As medical records should only ever be accessible to authorized personnel, HIPAA also demands the use of access controls - like usernames and passwords - to prevent said data falling into the wrong hands. Leaving faxes with PHI accessible to unauthorized parties leads to significant risks with regard to exposing protected information, security breaches and penalties. In some circumstances, such as the case of faxes delivered to email, two-factor authentication might also be sensible to prevent unauthorized sharing. Encryption is also a must, as it provides a method for stopping malicious users from intercepting data as it moves around the organization's network.

- **Auditing**

HIPAA mandates that all access to medical records leaves a paper trail. In the case of cloud fax, this precludes the possibility of sending patient information in plain text via email - organizations need a greater degree of visibility into how and when data is accessed, so a HIPAA-compliant cloud provider must ensure that every single attempt to open a confidential document is logged. An identification feature, such as a ribbon on faxes with unique identifiers, provides all of the metadata associated with the transmission including the time, date, sender, receiver and page count of transmitted documents, without storing any ePHI.

Retarus HIPAA Cloud Fax benefits:

Retarus understands that companies under the HIPAA regulations require enhanced security features. To do so, Retarus meets HIPAA requirements for security, backup, audit, access control and encryption by safeguarding information security and supporting audit trail for compliance. Data in transit is protected through HTTPS, FTP(S), TLS (SSL), and VPN. Security and encryption used for data at rest includes AES encryption, PGP and S/MIME, and X.590 certificate encryption for data storage and access via EAS. Additionally, further protection is taken at the network and physical level to ensure that various compliance and technology standards are met, including SSAE16 and ISAE3402 certifications.

Added restrictions are designed so that organizations can prevent employees from accessing sensitive data, as well as to prevent Retarus employees from viewing faxes that are sent or received. Using a patented technology, faxes are encrypted using a public key so that the images are only accessed by authorized personnel who have the private key installed on their work station or server. This prevents internal employees from forwarding confidential documents to non-authorized individuals. All fax images can be set to be encrypted on server at rest if the images are going to be stored after

Benefits for Organizations

- Compliant with HIPAA, HI-Tech regulations
- Reduce risk of HIPAA violations fines compared to on premise infrastructure
- Secure and reliable transmissions with Never-Busy offers higher deliverability and throughput rates over legacy technology
- Redundant data centers guarantees uptime for clients around the clock
- Detailed transmission reporting via web EAS portal provides optimized delivery, receipt, and tracking of sent and received information for compliance
- Lower operational costs through managed services
- Centralize communications for protected customer information
- Retarus enters into a Business Associate Agreement providing further level of protection
- SOC1 annual security audit completed ensures up to date standards
- 100% of Retarus US employees are HIPAA trained and certified

delivery, but to ensure HIPAA compliance, Retarus also provides immediate document deletion as soon as the document is transmitted to the recipient.

As Retarus' services and infrastructure are designed to keep organizations compliant with HIPAA, Retarus provides for centralized control and administration of fax communication across the entire organization as well as monitoring capabilities for fast troubleshooting and improved service. The Enterprise Administration Services portal provides a more in-depth level of compliance management through the ability to search for and return millions of records in milliseconds. It can focus on any specific message so that you can track the current status, number of pages, receiving fax number, and any of the processes that have been triggered. The Retarus fax infrastructure is designed so that it utilizes separate telecommunication grids and separate power grids to maintain a Hot/Hot, high availability environment where downtime is eliminated and critical messages can be processed regardless of outside factors.

With specialized services to the healthcare industry, including enhanced security to protect Patient Health Information in compliance with HIPAA and Hi-Tech laws, Retarus provides organizations with the flexibility to securely distribute virtually any document from any application using a centralized fax and delivery solution. With Retarus, the problems with manual faxing are immediately resolved; the system allows users to send and receive faxes directly from their email client or mobile devices, or integrate with their healthcare software applications to automate fax messaging completely in a user transparent manner that makes sending and receiving faxes an efficient, simple and cost effective process.

Retarus Secure Transmission Options:

Retarus Desktop Fax Services

With native integrations into email clients i.e. Microsoft Outlook, Lotus Notes, Office 365, and Office applications the Retarus platform allows for a more process as users are able to fax documents seamlessly from their desktop, minimizing errors, maximizing productivity and meeting HIPAA, PCI DSS and Hi-Tech compliance standards. Faxable documents like policies and authorizations are transmitted through Retarus, which eliminates error-prone, time consuming and repetitive manual processes.

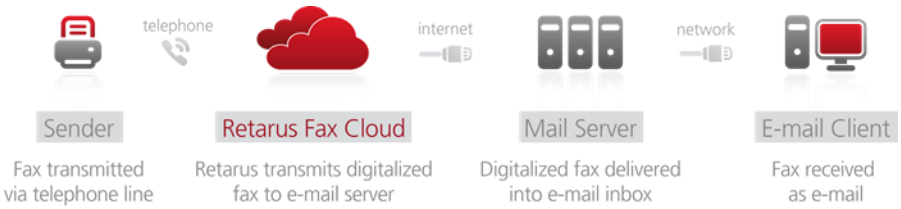
Desktop Services

Mail2Fax: Send faxes from any email system

Fax-to-Mail: Receive faxes directly to a desktop or applications

Fax for Exchange/Notes: Native integrated solution for Microsoft Exchange/Lotus Notes

Faxolution for Windows: Send faxes from Microsoft Office or any other Windows application



HIPAA Compliance Using E-mail:

- **Option 1:** Password Protected PDF File: - Fax is delivered to email as a PDF file that is password protected/encrypted. Here, users must key in the password to view the file

- **Option 2:** Exchange Transport Layer Security (TLS) turned on: Support for TLS Opportunistic or Forced. Account is setup to send faxes using Opportunistic/Forced whereby tokens are passed to secure connection. With forced TLS, both sides will have to exchange IP addresses/register so that there is a direct secure path to each other servers

- **Option 3:** PGP or X.509 Encryption Key: Customer buys encryption key and provides Retarus with the public Key and Customer configures private key in Adobe Reader. Adobe will open file if keys match

- **Option 4:** VPN Connection: Setup of VPN (Virtual Private Network) with both sides exchanging/registering IP addresses in order to make a secure point-to-point connection for delivery to client side server securely. The hosted service domain will be registered so when an email is addressed to that domain it will route directly through the VPN connection

Retarus Applications Fax Services

Integrates with any business applications - CRM, ERP, or legacy to send and receive critical messaging documents directly from business applications. Faxable items like policy requests, renewals, cancellations, etc. are transmitted seamlessely and efficiently through Retarus' integration to Insurance softwares.

HIPAA Compliance Using SFTP:

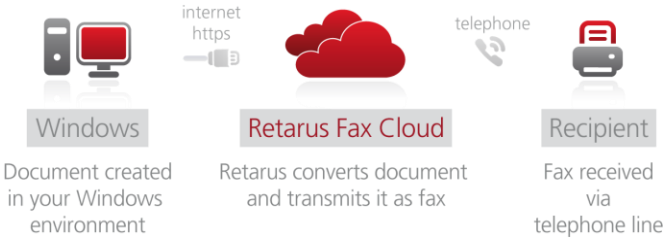
- **Option 1:** SFTP Push: Faxes can be pushed to clients SFTP Server using Secure File Transfer Protocol (SFTP) which requires customer to provide User ID/Password for connection. Documents then can be retrieved from this network drive internally to process downstream in the document workflow

- **Option 2:** SFTP Pull: Faxes can be pulled from Hosted SFTP Server using a provided a User ID/Password for connection. Documents then can be retrieved from SFTP Server and stored on customers network drive internally to process downstream in the document workflow. Or Customer can also use a security key to access the FTP server. This is similar to the key exchange in a PGP situation but in this case, customer provides public key to vendor who loads this on the server and the connection can only be made using the customer's private key. This setup is for Application interfaces where rules can be setup on when to pull the files from the hosted servers

HIPAA Compliance for Faxing Services

Faxolution for Windows

With Faxolution for Windows customers can efficiently send faxes directly from Microsoft Office or any other Windows applications. Faxolution for Windows is downloaded and stored locally on each user's desktop. Users can schedule times for fax deliveries and have access to fax transmission logs. The status of all fax jobs can be monitored at any time with just a click of the mouse.



HIPAA Compliance Using Fax to Printer:

Inbound faxes are sent directly to customer's defined local printer using a secure VPN Connection and mapping to access that printer remotely. Retarus also provides "Faxsolution for Windows" a secure print driver software that can be installed on each individual PC. Simply "Print" the document to the Faxsolution printer where the user will be prompted to enter in the fax number to send too. The Faxsolution software will then connect to the Retarus servers securely via an HTTPS connection using Retarus API calls to deliver the fax to the platform and then outbound to the fax machine.

HIPAA Compliance Using Web:

Access Faxes via Web through HTTPS connection: Portal access requires user name and password through HTTPS Secure connection. Fax images can be retrieved and store locally on client side PC or Network Drive. Users can create a fax message and attach a document through the web connection securely and send the fax directly from the portal.

Why Switch to Electronic Faxing?

Improve Organizational Compliance // Increase Message Deliverability Rate //
Greatly Reduce Operational Cost // Further Employee Efficieny // Provide Safer Transmissions
Gain Higher Satisfaction and Trust from Clients

About Retarus:

Retarus is a leading global provider of cloud based professional messaging solutions and has been developing and offering services for electronic corporate communications since 1992. The company's customers encompass large and medium-sized corporations, with service extending to more than 4,700 worldwide customers in various sectors. Customers such as Allianz, Bayer, Honda, Sony and Adidas rely on Retarus messaging services to exchange mission-critical business documents. Retarus and its affiliates employ more than 300 dedicated professionals worldwide. Each of its employees makes Retarus' core service values - customer focus, innovation, high quality and transparency - their mission.