HIPAA Compliant Faxing

A secure HIPAA (Health Insurance Portability & Accountability Act) compliant online fax solution for healthcare

We understand the sensitivities and the seriousness associated with keeping patient healthcare data private and secure. Which is why we have examined the details of all administrative, physical and technical safeguard specifications with preciseness, mitigating all HIPAA requirements to safeguard our customers' data, individuals' protected health information (PHI) and electronic protected health information (ePHI).

This is why eComfax is entrusted by healthcare providers, insurance companies and other covered entities to transmit their most sensitive documents.

The following eComFax HIPAA Compliance Statement aims to inform our customers who are "covered entities" under HIPAA that we are aware of their HIPAA requirements and will do our part to help ensure that their patient data is kept confidential. This Statement is not meant to take the place of a Business Associate Agreement.

Policies and procedures have been established to ensure our customers' data is kept confidential. These include (not limited to) the following:

Audit Control

eComFax uses multiple levels of audit control — from secure and automatic archiving of all faxes sent or received through eComFax for the life of your organization's account, to software and procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Data Encryption & Transmission Security

In order to comply with HIPAA you must pay careful attention to data that is in motion and at rest. All fax files at rest are encrypted using 256-bit Advanced Encryption Standard (AES). To protect data in transit between eComFax apps (currently mobile, API, or web) and our servers, we use Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption.

Highly Secure Data Centers

Our datacenters conform to the highest security standards (ISO 27001) and are part of the Cloud Security Alliance (CSA). They also conform to the OCF Level 1, having completed their Cloud Control Matrix which maps to the following selected frameworks: COBIT, HIPAA / HITECH Act, ISO/IEC 27001-2005, NISTSP800-53, FedRAMP, PCI DSSv2.0, BITS Shared Assessments, GAPP.

Information Security

We are always assessing risks and improving the security, confidentiality, integrity, and availability of our systems. We regularly review and update security policies, provide our employees with security training, perform application and network security testing (including penetration testing), conduct risk assessments, and monitor compliance with security policies.

Access Control

The eComFax virtual fax solution includes unique user identification, administrator privileges to grant and remove access, next generation (256-bit AES) encryption and other protocols to limit access to your organization's authorized personnel only. Inbound documents may be sent to only the intended recipient's email, limiting exposure and disclosure risks associated with faxing to a physical fax machine.

User Authentication

The eComFax service can be accessed by users via Email or online only with a valid username and password combination which are SSL encrypted. An encrypted session ID cookie is used to uniquely identify each user. While logged into our servers, all communications will be encrypted at all times.

Proper Disposal of Data

At the end of a Covered Entity's contract with eComFax, they may request their data to be deleted from the eComFax Servers. No printed reports or paper copies are ever retained in our facility. If reports are ever printed to further support the Covered Entity, they are shredded immediately upon completion of the task that required the paper output.

Other Privacy and Security Rules:

- Data backups stored in secured safe, world class data centers
- COMODO SSL Certificate (SSL/TSL creates a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption)
- 256 bit AES encryption on stored faxes
- Restricted outside access to all servers and production workstations
- Account owner authentication
- Sophisticated monitoring and escalation system
- Notice of data breach
- Report any non-compliance of which we become aware
- Automated virus checking
- Automated data backups
- Access to production systems is restricted with unique SSH key pairs, and security policies and procedures require protection of SSH keys. An internal system manages the secure public key exchange process, and private keys are stored securely.

- All employees receive training on our policies and procedures according to HIPAA mandates
- All employees complete thorough background checks and are required to sign a confidentiality agreement as part of their employment contract
- Named a HIPAA Security Official who creates, maintains, and trains regarding our HIPAA policies and procedures

Details of the HIPAA operation

For outgoing faxes, we accept TLS in email connections and can configure it as "mandatory", SecureFax / PciFax rejects SMTP communications that are not encrypted. Logically, the customer's mail service must also be HIPAA. In this case you can send faxes by email. The other possibility if your mail service is not HIPAA, is to do it through the web, since the connections are encrypted.

For incoming faxes: Faxes must be received by entering SecureFax / PciFax as incoming routing. With what is only sent a link that needs validation with credentials for consultation through the web portal.

Business Associate Agreement (BAA)

We sign Business Associate Agreement (BAA) with users of our Enterprise plan.