

MetroFax® HIPAA Statement

In August 1996, the Health Insurance Portability and Accountability Act (HIPAA) was signed into law. This legislation is designed to improve the portability and continuity of health benefits, to ensure greater accountability in the area of health care fraud, and to simplify the administration of health insurance.

This statement provides a summary of the policies and procedures that MetroFax has implemented to help protect data sent, received, and saved by MetroFax.

MetroFax as a "Business Associate"

MetroFax may function as a Business Associate to its customers. Per §160.103, a "Business Associate" is a person or entity that performs certain functions or activities on behalf of a covered entity involving use or disclosure of personal health information (PHI). Faxing PHI requires that both the covered entity and the Business Associate implement and follow security measures pursuant to HIPAA regulations.

Covered entities as defined by §164.501 are solely responsible for HIPAA compliance for their own purposes, regardless of their business relationship with MetroFax.

The information provided in this document does not constitute, and is no substitute for, legal or other professional advice. Users should consult their own legal or other professional advisors for individualized guidance regarding the application of the law to their particular situations, and in connection with other compliance-related concerns.

Administrative Safeguards

MetroFax has administrative actions, policies, and procedures, as well as provides training to its employees regarding safeguarding data and compliance with HIPAA regulations and the protection of personal health information (PHI). MetroFax personnel requiring access to any MetroFax network facility, equipment, system, or application that contains PHI must satisfy a user authentication mechanism such as a unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.

Customer data, including faxes sent, received, and saved on MetroFax services is protected and secure. It is only accessible by the account holder and authorized personnel for the purposes of system maintenance, monitoring, or compliance with legal or court orders. Faxes and their contents are the property and liability of the account holder.

Physical Safeguards

MetroFax utilizes physical measures, policies, and procedures to protect electronic information systems, facilities, and equipment from natural and environmental hazards including unauthorized intrusion. The MetroFax data center includes state-of-the-art redundant electrical power, cooling, and telecommunication facilities.

Our data center is a multi-layered secure facility that includes 24x7x365 manned security and checkpoints, closed circuit television (CCTV) cameras with continuous video recording of all entrances, exits, and data rooms. Servers are secured within card key-controlled access facilities with additional physical security protection. All egress and ingress activity into the MetroFax data center is restricted to a limited number of approved personnel and is recorded. Any additional personnel granted access to our data facilities are escorted at all times.

Technical Safeguards

MetroFax actively monitors its facilities and network infrastructure for intrusion using leading commercial security hardware and software. Access to the MetroFax servers is monitored 24x7x365 and all access is logged.

MetroFax requires that all accounts use a unique user identification, such as a username and password. For added security, credentials and data sent to and from customers are sent over the Internet via a secure channel using Secure Sockets Layer (SSL) technology. This is the same Internet transmission technology that is used for online banking and commerce.

APPLICATION SECURITY

When you send a fax with MetroFax from your existing email account, that email client's access controls are used, including your username and password. By using a strong password with your email account and regularly changing that password, the confidentiality of your fax data is protected from unauthorized persons.

When you use the MetroFax Fax Printer or use a Web browser to connect the MetroFax Dashboard all accounts must use a unique user identification, such as a username and password.

INTERNAL SYSTEMS SECURITY

MetroFax diligently protects the integrity of our internal network, including all hardware and software. All computers with access to our internal networks use username and strong passwords. All access is logged. In addition, we use leading third-party antivirus software that scans each computer, each accessed file, and all email messages. Antivirus software is frequently updated automatically to prevent the introduction of malicious code into our network infrastructure.

DATA ENCRYPTION

MetroFax uses strong encryption technology that helps to protect your online transactions. When you connect to the MetroFax Dashboard, data is encrypted at your computer and decrypted on the MetroFax servers using Secure Sockets Layer (SSL) technology. MetroFax uses the strongest commercially available encryption products including 128-bit VeriSign SSL Certification and 2048-bit RSA public keys. When you logon to your MetroFax account, a padlock icon appears in the Web browser indicating that SSL encryption is helping to protect your information.

MetroFax also supports Transport Layer Security (TLS) as an added encryption technology to help send secure information over the public Internet from your computer to the MetroFax servers. TLS is automatically enabled when your email service provider supports it. For increased security, dedicated point-to-point virtual private network (VPN) solutions are also available.

SERVER MANAGEMENT SECURITY

Customer data, including faxes sent, received, and saved on MetroFAX services is protected and secure. The data is only accessible by the account holder and authorized personnel for the purposes of system maintenance, monitoring, or compliance with legal or court orders. Faxes and their contents are the property and liability of the account holder.

Customer data is saved on secure systems that are behind firewalls with active intrusion monitoring and countermeasures.

A limited number of MetroFAX personnel have access to production servers, which are maintained in secure, limited access data centers with multiple layers of physical and electronic security. MetroFAX does not outsource the operation or maintenance of our production servers.

OPERATING SYSTEM SECURITY

MetroFAX maintains tight control of our service infrastructure and does not outsource the operation or maintenance of our production servers. A limited number of MetroFAX personnel have access to production servers, which are maintained in secure, limited access data centers with multiple layers of physical and electronic security.

In addition to regular security reviews of server logs and processes, we deploy software monitoring for attempted security breaches of our systems. To reduce potential security threats, we disable any service, protocol, user/group access accounts, and applications that are not required for the operation or maintenance of our systems.

A system of strong passwords that meet industry recommendations for length and complexity are regularly changed for each of our production servers. We do not maintain a common password database.

RELIABILITY AND BACKUP

Although uncommon, a failure in a component of the MetroFAX infrastructure should not significantly impact a customer's experience. Redundant components and infrastructure help to ensure a 99.9% availability of our services. Industry standard practices are followed for data provider redundancies, load balancing, and equipment failover scenarios.

MetroFAX utilizes physical measures, policies, and procedures to protect electronic information systems, facilities, equipment from natural and environmental hazards including unauthorized intrusion. The MetroFAX data center includes state-of-the-art redundant electrical power, cooling, and telecommunication facilities.

Customer data is maintained on geographically dispersed redundant disk-based storage to prevent catastrophic data storage failure.

MetroFAX has a disaster recovery plan in the unlikely event of an interruption to our primary services.