



faxing simplified. anytime. anywhere.

Protus Statement on HIPAA

Protus is committed to protecting the private health information you may transmit using MyFax®. Under the HIPAA (Health Insurance Portability & Accountability Act), Protus may be defined as a “Business Associate”. A “business associate” is a person or organization that performs certain services for a covered entity involving the use and/or disclosure of personal health information. When protected health information is faxed from a computer, HIPAA security measures need to be implemented by the covered entity and the business associate. According to the Security Standard Final Rule, a covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity’s behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.306(a) that the business associate will appropriately safeguard the information. This document is intended to provide assurance that Protus will safeguard all information faxed to and from covered entities while using the MyFax service. Protus has implemented both the physical, organizational and the technical safeguards necessary to protect the confidentiality and integrity of information being communicated using its MyFax services.

Protus Physical Safeguards

Protus’ fax production equipment is located at a facility that provides 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.

Protus Organizational Safeguards

The information contained in faxed documents is proprietary to the customer sending the fax. Protus employees do not have access to the Protus production equipment, except where necessary for system management, maintenance, monitoring, and backups. The Protus 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 Protus’ internal server environment remains protected and secure.

Protus Technical Safeguards

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, Protus monitors and analyzes firewall logs to proactively identify security threats.

Data Encryption

Protus leverages the strongest encryption products to protect “customer data and communications, including 128-bit Verisign SSL Certification and 1024 Bit RSA public keys. The lock icon in your internet browser indicates that data is fully shielded from access while in transit. Protus uses PGP security encryption and decryption software to secure electronic information. PGP is based on the use of an asymmetric Public-Key/Private-Key encryption algorithm, which is used to protect the confidentiality of a message, and ensure its authenticity and integrity.

User Authentication

Users can access the MyFax service via email or online only with a valid username and password combination, which is encrypted via SSL while in transmission. An encrypted session ID cookie is used to uniquely identify each user.

Application Security

Our robust application security model prevents one Protus customer from accessing another’s data. This model is reapplied with every request and enforced for the entire duration of a user session.

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.



Operating System Security

Protus 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.

Server Management Security

All data that is provided by a customer is owned by that customer. Protus employees do not have direct access to the Protus production equipment, except where necessary for system management, maintenance, monitoring, and backups. Protus does not utilize any managed service providers. The Protus 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 a primary tape library on a nightly basis. Backup tapes are immediately cloned to a second tape library to verify their integrity, and the clones are moved to secure, fire-resistant off-site storage on a regular basis. Disaster recovery plans are in place.

Sent faxes deleted after they are processed

Protus does not keep copies of single faxes on its production servers after delivery. Thus, confidential information contained in the faxes remains discrete.

Safe Faxing Tips

1. **Assess the recipient's security infrastructure:** Always ensure that the receiver has taken appropriate precautions to prevent anyone else from accessing the electronic or paperbased faxed documents.
2. **Confirm recipient's fax number:** Before sending a fax, check that the receiver's number is correct.
3. **Include a cover sheet:** Always complete a fax cover sheet that clearly identifies both the sender and the intended receiver. The cover sheet should include a standard confidentiality notice stating that the information contained in the fax is legally privileged, that the fax is intended for the named recipient only and a request to contact you directly if the transmission was sent in error.

Added security via Encryption - Optional

Install PGP software and provide Protus with your PGP Public Key: When a fax is sent to a MyFax customer, it first converts the fax to a TIFF file format. This TIFF file is then attached to an email and forwarded to the MyFax recipient. If the recipient has provided Protus with their PGP Public Key, Protus automatically encrypts the message using the recipient's Public Key before delivery. The recipient's PGP-enabled email software will then decrypt it for viewing. Complete, end-to-end security is provided through a fully automated, widely available, and easy-to-use process. Please contact Protus for more details on encrypting your faxes.

About MyFax

MyFax is the fastest growing Internet fax service used by individuals, small, medium, and large businesses to send and receive faxes using existing email accounts or the web. MyFax offers services in North America and Europe, including the United Kingdom, to industries recognized among the fastest growing adopters of internet fax including finance, insurance, real estate, healthcare, transportation and government. More than 15,000 new customers subscribe to MyFax each month. Additional information is available at www.myfax.com and www.myfax.uk.com.

Toll-free: 1-866-657-9885 | 613 733-0000 | Email: sales@myfax.com

© 2010 Protus®. All rights reserved. Protus®, MyFax® are trademarks of Protus®. Other trademarks referenced in this document are the property of their respective owners. Customers are solely responsible for ensuring regulatory compliance.