



## **Sfax™ HIPAA Security Overview**

### **The highest levels of security.**

Regulations protecting patient privacy are becoming ever more stringent. With manual and standard Internet fax products, security is virtually non-existent. Sfax adds security to both the sending and receiving of faxes. It also meets or exceeds all HIPAA security requirements.

Sfax provides added value for healthcare organizations to achieve HIPAA compliance through its high-performance document server with a central repository on which your organization can get Web-based access to your fax documents. Users gain universal access to these documents via https links.

### **Technically speaking, here's how Sfax works:**

#### **Sending Secure Sfaxes**

Sending secure Sfaxes is accomplished by using TLS, which is SSL (Secure Socket Layer) over the SSL port. TLS can be implemented on either a client-to-server or server-to-server basis. Because it is a standards-based service, Sfax can be used from almost any computer, operating system, PDA, or integrated into an existing software or service.

#### **Receiving Secure Sfaxes**

After an Sfax is received, a notification email will be sent to the email address or addresses you have registered with Sfax. The email will contain a link to the SSL Website. Sfaxes are password-protected and can only be viewed by registered users. Received faxes can also be accessed from a secure FTP server. Secure FTP access using SFTP (FTP over SSL) can also be enabled.

---