



EHR · Transcription · Speech Recognition

MxSecure, Inc.
17550 N. Perimeter Dr., Ste 250
Scottsdale, AZ 85255
(888) 580.1010
(480) 776.8980 fax

www.MxSecure.com

SECURITY and PRIVACY WHITEPAPER

Background and HIPAA Requirements

Maintaining the privacy and security of medical records is an extremely important duty and indeed one that is mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The HIPAA Privacy Rule requires covered entities (health plans, healthcare clearinghouses and healthcare providers) to make reasonable efforts to limit the use or disclosure of, and requests for protected health information (PHI) to the minimum necessary to accomplish the intended purposes.

The authorized uses of PHI are limited to those related to treatment, payment and healthcare operations (TPO).

The Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) has extended the Covered Entity requirements, including penalties and enforcement, Business Associates for Security and Privacy.

MxSecure Commitment

MxSecure, Inc. is committed to ensuring that all necessary policies, procedures and safeguards are in place at all times to comply with HIPAA Privacy and Security Rule requirements in the handling of protected health information in all areas of the company and with any and all business associates or sub-contractors that are permitted access to PHI.

Safeguards

HIPAA Security Safeguards fall into the following three categories:

- Administrative – including policies and procedures for ensuring security compliance.
- Technical – showing how the policies and procedures are implemented using technology controls such as authentication and audit trails.
- Physical – showing how the policies and procedures are implemented using physical controls such as firewalls, redundant computer servers, and biometric access entry to the data center.

I. Business Practices

- **HIPAA Compliance Management:** MxSecure has established a HIPAA Compliance Management Committee consisting of the CEO, CTO, and department director-level managers of the company. This committee is responsible for defining and enforcing compliance procedures and processes. Additionally, the CTO is the acting Privacy and Security Officer for MxSecure.
- **HIPAA Training:** All employees of the company attend formal annual training to ensure they understand the security requirements and are equipped to comply with all policies and procedures.
- **Confidentiality Agreements:** All employees of the company are required to sign a confidentiality agreement and non-disclosure agreement relating to PHI.
- **Business Associate Agreements with Contractors:** All contractors of the company with access to PHI must enter into a Business Associate Agreement that requires full compliance with all HIPAA requirements and all MxSecure privacy safeguards. In particular:
 - No contractor of the company is permitted to further sub-contract work for the company where PHI is involved unless such sub-contractor is contractually bound by the same policies, procedures, and safeguards as the contractor.
 - All contractors and sub-contractors must employ in-office staff and PHI may not be removed from office premises under any circumstances unless contractually and legally allowed.
 - All staff of contractors and sub-contractors with access to PHI must sign confidentiality and non-disclosure agreements that bind them to comply with HIPAA Privacy and Security Rules.

II. Workflow and Application Security:

- The MxTranscribe product includes the use of handheld digital recorders for voice capture. These voice files are electronically transmitted directly to MxSecure data center servers from customer sites using the proprietary MxTranscribe desktop application running on local PC's. The MxTranscribe application includes password-protected authentication prior to any transmission of files to or from MxSecure servers.
- The proprietary MxTranscribe desktop application applies 128-bit encryption to all files prior to any file transmission via the public Internet to the MxSecure data center servers.
- All use of the MxTranscribe or MxSecureMail web applications is forced to occur using the HTTPS protocol (SSL – secure socket layer) with 128-bit encryption strength. Attempts to access the application without SSL are redirected. (Read about SSL at: http://en.wikipedia.org/wiki/Secure_Sockets_Layer)
- Voice files are transmitted from MxSecure data center servers to production work centers via 128-bit SSL-secured web applications.

- During the processing of voice files to completed transcribed documents, only medical transcriptionists (MT) and quality control (QC) personnel are permitted access to files. Processes are in place to prevent unauthorized electronic transmission of these records to other parties. For example:
 - Access to the production floor is strictly limited to authorized personnel.
 - User authentication via unique user logins and passwords are required to access any file containing PHI.
 - Audit trails identifying all users who have accessed or edited PHI are maintained.
 - All floppy disk drives and USB ports are disabled to prevent copying of files to unauthorized media.
 - Internet access is limited and monitored.
 - The production process is operated as a paperless environment and network printer access is limited restricted.
 - All printed materials are shredded after their useful life, typically less than 24 hours.
 - All files containing PHI are removed from production floor PC's and servers after successful transmission to the MxSecure data center servers.
- Completed transcribed documents are returned to MxSecure servers from transcription work sites using the 128-bit SSL encrypted protocol.
- Customers retrieve completed files using the proprietary MxTranscribe desktop application.

II. Data Center Physical & Electronic Security:

This category includes safeguards to protect physical computer systems and related buildings and equipment from intrusion as well as fire and other environmental hazards. The use of locks, keys, and administrative measures used to control access to computer servers and facilities are also included.

- MxSecure servers and databases are housed in state-of-the-art tier one data centers with geographic redundancy. The data center is SAS 70 approved.
- The data center facilities provide a secure, climate-controlled environment that is operational 24 hours a day, 7 days a week, and 365 days a year.
- The data center is physically secured and requires the use of special biometric access (iris scans) to enter.
- Logs of all entry and exit from the facility are automatically maintained. Security personnel man the front desk 24/7/365.
- The data center facilities are equipped with climate control systems, fire detection and suppression systems, and backup UPS and generators.

- All MxSecure servers and databases are located on a secured internal network that is protected by Cisco Secure PIX Hardware Firewalls.
- MxSecure uses Microsoft SQL Server 2000 databases and implements the SQL Server Security Model. In summary, this model addresses security at multiple layers including securing access to the server, securing access to the database, securing access to database objects, and securing access through application roles.
- Access to the MxTranscribe system is limited to registered users. Users must provide their username and password to gain entry.
- A complete access audit trail is maintained including user session information. All database transactions are logged.