Medicine-On-Time IT Business Continuity and
Data Security
Created: 11/03/2015
Revised: 12/23/2015
Author: Peter H. Jenney
Version 1.1

INFORMATION SECURITY POLICY

Information & Physical Security

We at Medicine-On-Time (MOT) value our client's trust and are constantly evaluating our network and data environment to ensure we are taking reasonable and prudent measures to protect sensitive data including e-PHI specified by HIPAA. We have an ongoing process of evaluation that includes annual network security audits, monthly firewall vulnerability scans and active internal monitoring processes and applications. Additional measures include but are not limited to the following areas:

Employed Operating Systems

- Windows 10 Professional or newer
- Apple OSX 10.11 (El Capitan) or newer
- iOS 8 or newer
- Android 5.1 (Lollipop) or newer
- Windows Compact 8 or newer

Malware Protection

- Anti-virus protection
    - Windows Defender
    - Windows Edge
    - BitDefender (Mac)
    - Safari
    - Chrome

- Hard and Soft Firewalls
    - Network firewall that actively blocks attempted network attacks
    - Workstation firewall that actively blocks unauthorized access

- Vendor based security measures for systems potentially containing sensitive customer information including HubSpot, AccountEdge, ZenDesk and JIRA.

Email Security

Email is hosted in the Google Gmail domain which provides significant protection from spam, phish and other email-based malware. All employees must use either Microsoft Outlook 2016 or newer or Apple Mail 10.11 or newer, or Gmail using Google Chrome, Microsoft Edge, or Apple Safari each configured for "private" or "incognito" mode. No other email client is allowed for Medicine-On-Time email access.

Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) are employed to identify delivery source, enable non-repudiation of messages, and further help guard against phishing, spoofing and other email based attacks.

Where practicable, S/MIME certificates are employed to enable full email MUA to MUA (email client) encryption and signature verification.

Email clients are configured to use TLS/SSL connections in all cases to secure data in motion.

Email Retention

Google Apps Vault provides data preservation and legal search across Google Apps and includes a default email retention policy of 6 years for messages that have been deleted from a users mailbox and indefinitely for active messages.

Physical network and data security

- There are no on premise data, application or other servers
- Access to virtual servers limited to key personnel authorized by Management

Logical network and data protection

- Only encrypted data sessions are allowed for remote network access.
- Internal access to client data by MOT employees on a need-to-know basis.
- File access auditing (Google Drive, Microsoft OneDrive)
- Annual staff training for network/data security awareness and best practices
- Secure Data Backup, Offsite Storage, Cloud Storage, Encrypted Backups, Period, Recovery Time, Restore to Alternate Servers, and Amazon AWS snapshots.

PC Security

- All systems have full volume encryption turned on to secure data at rest
- Password format is minimum 16 characters, at least 1 lower and one upper case character, at least 1 number and at least 1 "special" character.
- Passwords are maintained on each system using LastPass and include all internal and all cloud passwords.

Mobile Device Security

- MOT IT supports Bring Your Own Device (BYOD) but all devices are required to have the same level of data encryption and password strength
- Where possible, mobile devices should employ self destruct mechanisms where multiple incorrect login attempts cause the system to erase its data
- Where possible, mobile devices should support remote destruct whereby stolen or lost devices can be wiped clean.

Physical building security

- All physical entrances to the building are secured and logged.
- Access system plus building security system.

Business Associate Agreements (BAA)

Medicine-On-Time's business is software and regulated data; and as such we have and will continue to enter Business Associate Agreements (HIPAA Definition) with partners and vendors to provide software products and services to our clients. All Business Associate Agreements are dually signed and stored electronically and accessible in compliance with this MOT Information Security Policy.

References

HHS.Gov - http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html