HIPAA-20: Endpoint Computer Security Policy

Effective Date:	7/1/2018	Last Revised:	6/21/2018

Scope of Policy

This policy governs Endpoint security for all TCS Servers and Desktop/Laptop Computers for **TCS**. All personnel of **TCS** must comply with this policy. Demonstrated competence and compliance with the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Assumptions

- **TCS** must comply with HIPAA and the HIPAA implementing regulations pertaining to protection from so-called malware, in accordance with the requirements at § 164.308(a)(5).
- The use of appropriate techniques, technologies, and methods to update critical security patches and protect information systems from malicious software ("malware") is a proven approach to reducing the likelihood of data breaches, system malfunctions, and HIPAA violations.

Policy Statement

Effective compliance with HIPAA Security Rule requires that TCS implement and maintain an appropriate endpoint security policy and procedures. The purpose of this policy is to ensure that all workforce members understand the importance of maintaining updated security patches and endpoint security software definitions on their assigned desktop/laptop computers, as well as all Servers.

- Workstations and other computer systems are provided to employees for the purpose of performing their job functions. Employees shall be responsible for using workstations appropriately in conformance with this Policy. *This shall include following TCS's standard policy and procedures to maintain effective desktop security*.
- An effective security patch management process will be maintained to ensure that security patches are applied to all workstations, servers and portable devices, where feasible. Leading third party applications (i.e., browsers, Adobe, Java, etc.) will also be included in the TCS patch management process as well to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected. Any other applications should be manually updated with any new security patches released.
- An approved endpoint security (anti-virus / anti-malware) software that protects against malicious software will be deployed and maintained on all workstations, servers and portable devices. The Endpoint Security software must be current and up to date with new virus / malware definitions. Employees must use and keep active current versions of approved anti-virus / anti-malware software scanning tools to detect and remove malicious software from workstations and files. Employees must not disable these tools unless specifically directed by computer support personnel to do so in order to resolve a particular problem.
- Security Awareness Training shall include information on emerging cybersecurity concerns, and associated email threats.
- Workforce members shall comply with all TCS training regarding security best practices at all times, including accessing any public Wi-Fi connections, and being aware of man-in-the-middle threats.
- Responsibility for enforcement of this policy shall reside with the Executive Director, in consultation with the appropriate IT personnel, who shall ensure that the most effective and appropriate techniques, technologies, and methods are continuously used to protect our information systems, and the individually identifiable health information they contain, from security threats.
- It is the Policy of **TCS** to fully document all endpoint protection-related activities and efforts, in accordance with our Documentation Policy.

Procedures:

- ❑ Endpoint security software will be installed, monitored, and maintained by designated IT personnel, who will be responsible for reporting status of efforts and issues to Security Officer and/or Executive Director on a regular basis.
- ❑ A management agent will be installed on all workstations in order to manage the deployment of approved security patches as well as monitoring the status of endpoint security updates.
- ❑ Both of these processes required staff computers to be left on overnight while connected to the internet. If there is not time for updates during normal work hours, then the computer should be left one or more nights a week pursuant to instructions provided by the Executive Director or the IT Staff.
- ❑ Any remote access to the TCS network shall require an approved VPN client.