HIPAA-31: Facility Security Policy

Effective Date:	12-01-2015	Last Revised:	7-17-2017

Scope of Policy

This policy governs Facility Security for **TCS**. All personnel of **TCS** must comply with this policy. Demonstrated competence in 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 facility security, in accordance with the requirements at § 164.310(a)(1-2).
- In addition to other technical and administrative safeguards, strong facility security is an essential element of our efforts to provide protection for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **TCS** to provide strong facility security, in addition to other technical and administrative safeguards, in order to provide protection for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of **TCS** to fully document all facility security-related activities and efforts, in accordance with our Documentation Policy and our Maintenance Records Policy.
- It is the Policy of **TCS** to fully document facility security maintenance records-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- Primary responsibility for facility security is hereby assigned to Executive Director, who shall analyze the security of our facility and implement devices, tools and techniques to strengthen our facility to a reasonable level, to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- A periodic analysis of our facility security controls should include, but are not limited to, the following factors:
    - Windows and door access point
    - Management of Locks and keys
    - Electronic access control systems (i.e., Building Alarms, Video Surveillance)
    - Auditable access logs for after-hour access
    - Routine and non-routine deliveries
    - Computer equipment and wiring center rooms
- Responsibility for the creation and updating of facility security maintenance records is hereby assigned to Security Officer, who shall establish procedures for maintaining such records in appropriate form.
- Any staff member who discovers a facility security vulnerability/risk shall bring it to the attention of the Security Officer immediately.

- **IT Equipment Security**
    - All TCS servers, and network hardware are maintained in secured, locked, environmentally conditioned rooms with 24 hour per day monitoring devices which alert the Network

Administrator and/or Security Officer of any problems. Access to these rooms is limited to authorized IS and facility services workforce as required to perform job responsibilities to maintain these rooms and/or the equipment within these rooms. Access by anyone else is granted only by approval from the Executive Director and only with an escort by an authorized IT or facility services workforce member.

- Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities. Third parties may be authorized by the Security Officer or Executive Director to access systems/applications on an as needed basis.
- All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
- Permanent Workstations (i.e. desktop computer, printers, and monitors) may only be moved by authorized IT workforce members.
- All wiring associated with a workstation may only be installed, fixed, upgraded, or changed by an authorized IT workforce member or other individual authorized by the Executive Director.

❑ **System/Application Access Control**

- All systems/applications purchased by **TCS** are the property of **TCS** and are distributed to users by the Information Systems staff only.
- Prior to downloading, all software must be registered to **TCS** and must be approved in advance by the Executive Director and the IT department. To prevent computer viruses from being transmitted through **TCS'**s information systems, there will be no unauthorized downloading of any unauthorized software.
- The Information Systems staff is responsible for downloading all upgrades, testing upgrades, and for supporting **TCS** systems/applications.