HIPAA-07: Assignment of Security Responsibility Policy

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

Scope of Policy

This policy governs the Assignment of Responsibility for health information data 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 the assignment of security responsibility, in accordance with the requirements at § 164.308(a)(2).
- The assignment of overall security responsibility is an important and integral part of our overall risk management process, and shall be conducted in accordance and coordination with our Risk Management Process Policy.

Policy Statement

- It is the Policy of **TCS** to fully document the assignment of overall security responsibility, and all related activities and efforts, according to our Documentation Policy and HIPAA requirements
- It is the Policy of **TCS** to assign overall responsibility for the security of individually identifiable health information, in electronic and other forms, to a person who is qualified and competent to assume such responsibility.
- The person with overall responsibility for the security of individually identifiable health information, in electronic and other forms, shall be the Security Officer, who shall report directly to the Executive Director. This person shall also work in conjunction with the TCS HIPAA Compliance Committee and other IT staff consultants to address the provisions of the HIPAA Security Rule.
- Appropriate training and support services shall be provided to the Security Officer to ensure he/she is kept abreast of evolving security issues and requirements.

Procedures

The HIPAA Security Officer, in consultation with the Executive Director, shall implement the following procedures, as appropriate, in accordance with **TCS**'s Risk Management policies:

- Periodically review the list of all individuals who have access to the Practice's confidential information, including PHI.
- Cooperate with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- Work with appropriate technical personnel to protect the Practice's confidential information from unauthorized use or disclosure.
- Develop specific policies and procedures mandated by the Security Rule.
- Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with HIPAA Rules to safeguard PHI, and ensure that the Practice's confidential data is adequately protected when such access is granted.

This review and oversight should include ensuring that current Business Associate Agreements are executed by appropriate vendors and maintained on file.

- ❑ Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- ❑ Ensure that future Practice initiatives are structured in such a way to safeguard ePHI.
- ❑ Oversee periodic system audits and ensure remedial action is taken as necessary and authorized by the TCS HIPAA Compliance Committee.
- ❑ Oversee employee security awareness training and testing.
- ❑ Remain up-to-date and advise on new technologies to safeguard ePHI.
- ❑ Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice's policies and procedures as necessary.
- ❑ Monitor any data sharing initiatives for compliancy.