HIPAA-40: Data Integrity Controls Policy

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

Scope of Policy

This policy governs Data Integrity Controls 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 data integrity controls, in accordance with the requirements at § 164.312(c)(1-2).
- □ The purpose of this Integrity Controls Policy is to ensure that electronic Protected Health Information ("PHI" and "ePHI", as defined by HIPAA) has not been altered or destroyed in an unauthorized manner.
- □ The establishment and implementation of an effective data integrity controls policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- □ It is the Policy of **TCS** to establish and maintain appropriate and effective data integrity controls in full compliance with the requirements of HIPAA.
- □ Responsibility for the development and implementation of this data integrity controls policy, and any procedures associated with it, shall reside with the Executive Director in collaboration with appropriate IT personnel, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- □ Specific procedures shall be developed to specify the proper usage and application of data integrity controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- □ It is the Policy of **TCS** to fully document all data integrity controls-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- □ Integrity is the process of protecting data from improper alteration or destruction during transit. Digital signatures and Message Digest (One-way Hash) both allow for the assurance that electronic PHI is truly from the sending entity and has not been modified.
- □ Integrity controls that focus on electronic PHI while in transit are designed to assure data is not properly modified until it reaches its appropriate destination or is disposed of. Technical solutions that assist in preserving data while in transit may include: use of firewalls, VPN's cryptography, and other authentication devices.