

HIPAA-42: Data Transmission Security Policy

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

Scope of Policy

This policy governs Data Transmission 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 data transmission security, in accordance with the requirements at § 164.312(e)(1) and § 164.312(e)(2).
- The purpose of our Data Transmission Security Policy and Procedures is to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
- The establishment and implementation of effective Data Transmission Security Procedures is a crucial element in our overall objective of 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 implement technical security measures to guard against unauthorized access to Electronic Protected Health Information that is being transmitted over an electronic communications network, in full compliance with the requirements of HIPAA.
- Responsibility for the development and implementation of these Data Transmission Security Procedures shall reside with the Executive Director in collaboration with appropriate IT personnel, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
- Specific Data Transmission Security Procedures shall be developed to protect individually identifiable health information, including Electronic Protected Health Information ("E PHI", as defined by HIPAA).
- It is the Policy of **TCS** to fully document all Data Transmission Security Procedures, activities, and efforts, in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

- TCS** utilizes secure VPN (virtual private network) connections whenever transmitting electronic PHI.
- TCS** transmits all company-based email through a secured email server.
- TCS** utilizes email encryption for transmission of any messages or documents containing ePHI.
- Electronic PHI is permitted only in the body of secure, intra-agency emails.
- At no time is PHI permitted in the subject line of any email.
- No texting of electronic PHI is permitted at any time.