HIPAA-38: Encryption and Decryption Policy

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

Scope of Policy

This policy governs the Encryption and Decryption of Protected Health Information 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 encryption and decryption, in accordance with the requirements at § 164.312(a) (1-2).
- ❑ The establishment and implementation of an effective encryption and decryption 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 this encryption and decryption policy in full compliance with all the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of this encryption and decryption 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 encryption and decryption for all computers and workstations 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 encryption and decryption-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- ❑ Encryption of Data at Rest:
  - Commercial grade data encryption technology should be installed and maintained on all mobile communication or portable storage devices (e.g., laptops, tablets, iPADS, Cell Phones, thumb drives, flash drives, etc.) which can have access to ePHI or other confidential data.
  - The use of any fileshare applications (e.g., Drop Box, Google Drive, iCloud, Microsoft OneDrive, etc.) shall not be used without approval of the Executive Director in collaboration with IT personnel. Such approval will only be granted if: 1) the filesharing need is necessary for business operations; 2) the remote parties involved have a current BAA on file; and all data is encrypted prior to sharing; or 4) the filesharing service provides commercial grade encryption and security and will sign a current BAA.
  - Off-site backup media should be encrypted at all times including any electronic transmission solution utilized.
- ❑ Data Transmission Security:
  - a) Any ePHI or other confidential data shall be sent via email or any other communications technology unless it is fully encrypted using appropriate encryption technology.
  - b) Any use of other data transmission (FTP, etc.) shall not be allowed unless encryption or other appropriate security protocol has been approved by the Executive Director in collaboration with IT personnel.
- ❑ Guidelines for the use and maintenance of approved encryption technology will be communicated to all involved staff and vendors.