

# HIPAA-41: Person or Entity Authentication Policy

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

## Scope of Policy

This policy governs Authentication of Persons or Entities seeking access to Electronic Protected Health Information in the possession of **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 person or entity authentication, in accordance with the requirements at § 164.312(d).
- The purpose of this Person or Entity Authentication Policy is to ensure that electronic Protected Health Information ("PHI" and "ePHI", as defined by HIPAA) can only be accessed by persons or entities who are in fact who they claim to be, and not imposters.
- The establishment and implementation of an effective Person or Entity Authentication Policy 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 maintain this Person or Entity Authentication Policy in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this Person or Entity Authentication 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 authentication of persons and entities who request access to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) on our computers, workstations and systems.
- It is the Policy of **TCS** to fully document all person or entity-related activities and efforts, in accordance with our Documentation Policy.

## Procedures

- Each employee is issued a unique use ID and password permitting role-based access to electronic PHI.
- Passwords are deactivated promptly for employees no longer authorized to access such information.