HIPAA-22: Password Management Policy

Effective Date:	12-01-2015	Last Revised:	10-18-2017

Scope of Policy

This policy governs information systems Password Management 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 password management, in accordance with the requirements at § 164.308(a)(5).
- The creation and management of strong passwords is one of the simplest and most effective methods of protecting access to electronic systems containing, transmitting, receiving, or using individually identifiable health information.
- The use of an approved Password Manager is also an effective method for generating and securing complex passwords for multiple systems.

Policy Statement

- It is the Policy of **TCS** to require the use of strong and complex passwords by all workforce members who access, use, or maintain systems that contain, transmit, receive, or use individually identifiable health information.
- The responsibility for implementing this policy and any attendant procedures is hereby assigned to the Executive Director, who shall develop and implement this policy in coordination with the most senior information technology personnel.

Procedures

- All passwords used to access systems containing, transmitting, receiving, or using individually identifiable health information shall be a minimum of ten (10) characters in length, and should include non-alphanumeric characters or symbols in them.
- Passwords should be changed by users at least once every twelve (12) months.
- In the event of an information system compromise, as determined by the designated HIPAA Official or HIPAA Officer, some or all workforce-member passwords may need to be changed. This determination shall be made by the most senior IT personnel in consultation with the Executive Director.
- Under no circumstances shall passwords be written down and kept at or near computers and workstations where they may be found by others. Passwords may, however, be written down and stored in a workforce member's wallet or purse, if the password is thus afforded protection equal to the protection afforded to workforce members' cash, credit cards, and other critical documents.
- Any workforce member who loses, misplaces, forgets, or experiences any compromise of their password shall immediately notify HIPAA Security Officer, or, if they are unavailable, shall notify the Executive Director. Such notification of password compromise must be made *immediately* to the contact(s) indicated herein, but in no case shall such notification be delayed more than one (1) hour.
- Proper password management shall be emphasized in HIPAA training programs, in security reminders, and in any HIPAA security awareness resources used by this organization.