HIPAA-21: Log-In Monitoring Policy

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

Scope of Policy

This policy governs Log-In Monitoring 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 log-in monitoring, in accordance with the requirements at § 164.308(a)(5).
- □ Regular monitoring of log-ins and log-in attempts is a proven approach to controlling access to sensitive information systems and data, and to detecting inappropriate information systems activity.
- □ The monitoring of successful and unsuccessful Log-In attempts is also a well established method of detecting malicious intrusions, and intrusion attempts, into information systems by unauthorized persons.

Policy Statement

- □ It is the Policy of **TCS** to establish a program of regular monitoring and review of log-ins and log-in attempts.
- □ The HIPAA Security Officer, in consultation with appropriate IT personnel, shall assume responsibility for ensuring appropriate monitoring and analysis of log-in attempts occurs that such activities are executed on a continuous and ongoing basis.
- □ Discrepancies and potentially inappropriate or illegal activities shall immediately be brought to the attention of senior management, legal counsel, and/or Human Resources, as appropriate.
- □ It is the Policy of **TCS** to fully document all log-in monitoring-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- □ TCS shall develop, implement, and regularly review a formal, documented process for monitoring login attempts and reporting discrepancies.
- □ Access to all information systems must be via a secure login process. At a minimum, the process should:
  - Validate login information only when all data has been input. If an error occurs, the system must not indicate which part of the data is correct or incorrect.
  - Limit the number of unsuccessful login attempts allowed.
  - Include the potential use of multiple challenge questions if a password is forgotten to aid in password reset.
- □ Information systems' login process should include the ability to:
  - Record unsuccessful login attempts.
  - After a specific number of failed login attempts, enforce a time delay before further login attempts are allowed or reject any further attempts without authorization from an appropriate workforce member.
  - Limit the maximum time allowed for the login process.