HIPAA-15: Information Systems Activity Review Policy

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

Scope of Policy

This policy governs Information Systems Activity Reviews 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 information systems activity review, in accordance with the requirements at § 164.308(a)(1).

Policy Statement

- ❑ It is the Policy of **TCS** to regularly review various indicators and records of information system activity, including, but not limited to: audit logs; access reports; and security incident reports.
- ❑ The goal of this Information Systems Activity Review Policy is to prevent, detect, contain, and correct security violations and threats to individually identifiable health information, whether in electronic or any other forms.
- ❑ It is the Policy of **TCS** to fully document all information system activity review activities and efforts.
- ❑ This Information Systems Activity Review Policy shall be implemented and executed in accordance with our risk management policies and procedures.

Procedures

- ❑ The Network Systems Administrator shall review Security Event Logs, System Access Rights and Auditable Access Logs no less than monthly.
- ❑ The Network System Administrator shall log any pertinent findings and submit a monthly report to the HIPAA Compliance Committee that provides a summary recap of any findings and status of any remediation.
- ❑ Monthly Log Reviews and Quarterly Vulnerability Scans will be conducted by the Network Administrator. Printed reports generated will be stored in a binder in TCS's administrative office.