HIPAA-26: Contingency Operations Policy

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

Scope of Policy

This policy governs Contingency Operations planning and implementation 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 contingency operations, in accordance with the requirements at § 164.310(a) (1-2).
- Contingency Operations, for purposes of this policy document, are defined as processes and procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
- Contingency operations plan and procedures, in combination with other emergency preparedness plans and procedures, shall be documented, analyzed, revised and updated periodically in accordance with other established emergency preparedness and documentation policies and procedures.

Policy Statement

- It is the Policy of **TCS** to be fully prepared to protect individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), during emergencies and contingency operations.
- Responsibility for planning and executing contingency operations shall reside with Executive Director, who shall prepare, review, and update plans for contingency operations on a periodic basis.
- The primary purpose of our contingency operations procedures is to allow our organization to restore lost data in the event of an emergency.
- It is the Policy of **TCS** to fully document all contingency operations plans and procedures, in accordance with our Documentation Policy.

Procedures

- Emergency and contingency plans are the responsibility of the Executive Director, who shall ensure that all such plans are up-to-date and meet our emergency preparedness requirements.
- Emergency and contingency plans, as well as data backup and disaster recovery plans shall be reviewed, and revised if necessary, at least annually. Copies of all such plans shall remain on file and be available to all personnel.
- The Executive Director shall fully document all emergency preparedness plans, including emergency and contingency plans, backup and disaster recovery plans and all the revisions thereto, in accordance with our Documentation Policy and the requirements of HIPAA.
- Service Level Agreements will be executed as needed with appropriate vendors providing any facilities, equipment or support services for the emergency and contingency plans developed.