HIPAA-28: Data and Applications Criticality Analyses

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

Scope of Policy

This policy governs Data and Applications Criticality Analyses 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 the analysis of the relative criticality of both data and applications, in accordance with the requirements at § 164.308(a)(7).
- A thorough assessment and understanding of the relative criticality of both data and applications is essential to emergency preparedness, and to effectively protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) during emergencies and during normal business operations.

Policy Statement

- It is the Policy of **TCS** to assess the relative criticality of all data, so that such data may be properly protected during emergencies and during normal business operations.

Procedures

- Data to be subject to criticality analysis shall include individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- Criticality analysis shall be the responsibility of the Executive Director or designees, who shall work in cooperation with legal counsel and other internal parties as necessary to execute and document such analyses.
- Criticality analyses shall determine and document the relative criticality of each type or category of data and applications that **TCS** possesses and/or uses to the continuity and success of our operations.
- The most critical data and applications shall be given the given the highest priority in terms of investment and emergency protection preparations; with less critical categories or types of data and applications receiving proportionately less funding and attention, as appropriate.
- In conducting data and applications analyses, the Executive Director or designees shall employ the technical guidance and recommendations of the National Institute of Standards and Technology ("NIST"), and/or other information technology "best practices", as appropriate.
- All analyses of the relative criticality of both data and applications shall be fully documented in accordance with our Documentation Policy and the requirements of HIPAA.