HIPAA-23: Security Incident Procedures

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

Scope of Policy

This policy governs responses to Security Incidents involving the breach or compromise of Protected Health Information 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 security incident procedures, in accordance with the requirements at § 164.308(a)(6) and at § 164.400 to 164.414.
- Appropriate responses to security incidents may include, but are not limited to:
  - Rapid identification and classification of the severity of security incidents.
  - Determination of the actual risk to individually identifiable health information, and the subject(s) thereof.
  - Repairing, patching, or otherwise correcting the condition or error that created the security incident.
  - Retrieving or limiting the dissemination of individually identifiable health information, if possible.
  - Determining if the security incident rises to the level of a reportable breach under the HIPAA regulations.
  - Making a lawful and appropriate report of a breach, if required, to the appropriate parties. Appropriate parties to whom breaches must be reported, as defined by HIPAA regulations, may include, but are not limited to: *Patients, Consumers, Regulatory Authorities, including HHS and/or the Federal Trade Commission Law Enforcement and the local media, if necessary and required by law.*
  - Mitigating any harmful effects of the security incident.
  - Fully documenting security incidents, along with their causes and our responses.
  - Expanding our knowledge of security incident prevention, through research, analyses of security incidents, and improved training and awareness programs for workforce members.
- Compliance with HIPAA's data protection requirements is mandatory and failure to comply can bring severe sanctions and penalties.

Policy Statement

- It is the Policy of **TCS** to rapidly identify and appropriately respond to all security incidents, regardless of their severity.
- Responsibility for responding to and managing security incidents shall reside with HIPAA Privacy & Security Officers in consultation with the Executive Director.
- It is the Policy of **TCS** to fully document all security incidents and our responses thereto, in accordance with our Documentation Policy and HIPAA requirements.

Procedures

- All employees will be trained on HIPAA related policies, including the requirement to report anything determined to pose a risk, regardless of the severity, to the security of PHI. Such training will occur at New Hire Orientation and annually thereafter.
- When a security incident is reported, the details of the incident will be fully documented, as well as any follow-up efforts or notifications made as deemed appropriated and necessary by the HIPAA Privacy and Security Officers in consultation with the Executive Director.