HIPAA-13: Risk Management Process Policy

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

Scope of Policy

This policy governs the establishment and maintenance of a Risk Management Process for **TCS**. This Risk Management Process Policy shall encompass a comprehensive range of activities including an incorporated Risk Analysis and Annual Security Risk Management Plan.

Two key principal components involved in the risk management process are Risk Analysis and Risk Management Process:

- **Risk Analysis:** 164.308(a)(1)(ii)(A) R - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) held by the covered entity.
- **Risk Management:** 164.308(a)(1)(ii)(B) R - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with *164.306(a).

Assumptions

- **TCS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the establishment and management of an appropriate risk management process, in accordance with the requirements at § 164.302 to § 164.318.
- The establishment and maintenance of an appropriate risk management process will generally reduce our privacy and security risk, can reduce the likelihood of creating HIPAA violations, whether inadvertent or intentional.

Policy Statement

- It is the Policy of **TCS** to establish, implement, and maintain an appropriate Risk Management Process. This Policy shall include a periodic Risk Analysis and annual Risk Management Plan as integral components in the Risk Management Process.
- **Risk Management Process** - Our risk management process shall strive to identify, analyze, prioritize, and minimize identified risks to information privacy, security, integrity, and availability. The nature and severity of various risk and risk elements shall be identified and quantified, with the goal of reducing risk as much as is practicable. The risk management process shall be ongoing, and shall be updated, analyzed, and improved on a continuous basis.
- **Risk Analysis** – A Risk Analysis is an integral part of the organization's overall Risk Management Process Policy and process and shall be conducted periodically in order to assess potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information ("ePHI") that the organization has been entrusted with.
- **Risk Management Implementation** – Upon completion of each Risk Analysis conducted, an associated Risk Management implementation plan shall be developed. This plan will include a list of any HIPAA security gaps identified with associated recommendations to remediate risks. It shall be the responsibility of the Executive Director working with the HIPAA Officials to prioritize issues be remediated within a specific timetable. Any HIPAA compliance gaps or vulnerabilities identified that are not approved for remediation shall be documented in the plan with explanation for cause and acknowledgement of residual risk assumed on behalf of the organization.
- The results of the risk management process shall be input into management's decision-making processes, in order to help reduce our overall risk and to comply with HIPAA and other applicable laws and regulations.

- ❑ The risk management process shall be under the direct control and supervision of the Executive Director, and shall involve legal counsel, information technology, and any other parties or persons deemed to be appropriate to the process.
- ❑ Responsibility for conducting periodic risk analyses shall be with the designated HIPAA Security Officer, in consultation with the agency's Executive Director, in consultation with IT consultants and the HIPAA committee, who shall establish a plan and procedures for the conduct of such analyses.

Procedures

- ❑ Feedback will be solicited from all employees surrounding perceived risks to information privacy, security, integrity, and availability.
- ❑ Any identified risks will be investigated and mitigated accordingly.
- ❑ Privacy-related risks will also be considered during the updating of the agency's Risk-Management Plan, which occurs annually.
- ❑ Risk analyses and assessments shall be conducted annually and as deemed necessary by the HIPAA Committee.
- ❑ The results of risk analyses and assessments shall become an integral part of management's decision-making process, and shall guide decisions related to the protection of Protected Health Information.
- ❑ All such risk analyses and assessments shall be documented in accordance with this organization's Documentation Policy and HIPAA Regulations.
- ❑ The specific mitigation measures identified will be implemented in the most expeditious manner possible to minimize the risk of additional or increased vulnerability in the future.
- ❑ Follow-up efforts will be employed to ensure mitigation measures had the desired effect.