Policy Number: SHI-PP-020
Effective Date: Jan 01, 2020
Last Revised: _____

Assignment of Security Responsibility Policy

Introduction

STRATEQ HEALTH, INC. has adopted this Assignment of Security Responsibility Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).

STRATEQ HEALTH, INC. hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs the Assignment of Responsibility for health information data security for **STRATEQ HEALTH, INC**. All personnel of **STRATEQ HEALTH, INC.** 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.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Assumptions

- **STRATEQ HEALTH, INC.** hereby recognizes its status as a Business Associate under the definitions contained in the HIPAA Regulations.
- **STRATEQ HEALTH, INC.** must comply with HIPAA and the HIPAA implementing regulations pertaining to the assignment of security responsibility, in accordance with the requirements at § 164.308(a)(2).
- The assignment of overall security responsibility is an important and integral part of our overall risk management process, and shall be conducted in accordance and coordination with our Risk Management Process Policy.

Policy Statement

- ❑ It is the Policy of **STRATEQ HEALTH, INC.** to assign overall responsibility for the security of individually identifiable health information, in electronic and other forms, to a person who is qualified and competent to assume such responsibility.
- ❑ The person with overall responsibility for the security of individually identifiable health information, in electronic and other forms, shall be the Privacy Officer who shall report directly to the CTO of the company.

Procedures

The Privacy Officer shall implement the following procedures, as appropriate, in accordance with **STRATEQ HEALTH, INC.**'s Risk Management policies:

- ❑ Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with Human Resources, the information security officer, administration, and legal counsel as applicable.
- ❑ Maintain an accurate inventory of (1) all individuals who have access to the company's confidential information, including PHI, and (2) all uses and disclosures of the company's confidential information by any person or entity.
- ❑ Administer patient requests and processes under HIPAA's patient rights.
- ❑ Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- ❑ Cooperate with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- ❑ Work with appropriate technical personnel to protect the company's confidential information from unauthorized use or disclosure.
- ❑ Develop specific policies and procedures mandated by the Privacy Rule.
- ❑ Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- ❑ Draft and disseminate the privacy notice required by the Privacy Rule.
- ❑ Determine when the Practice might need member consent or authorization for use or disclosure of PHI, and draft forms as necessary.
- ❑ Ensure that any research efforts conducted or supported by the Practice comply with appropriate privacy laws and policies and adequately protect the privacy of the data subjects.
- ❑ Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with the Privacy Rule, and ensure

that the Practice's confidential data is adequately protected when such access is granted.

- ❑ Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- ❑ Ensure that future company initiatives are structured in such a way to ensure patient privacy.
- ❑ Conduct periodic privacy audits and take remedial action as necessary.
- ❑ Oversee employee training in the area of privacy.
- ❑ Guard against retaliation against individuals who seek to enforce their own privacy rights or those of others.
- ❑ Remain up-to-date and advise on new technologies to protect data privacy.
- ❑ Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice's policies and procedures as necessary.
- ❑ Track pending legislation regarding data privacy and if appropriate seek to influence that legislation.
- ❑ Anticipate members' concerns and questions about the company's use of their confidential information and develop policies and procedures to respond to those concerns and questions.
- ❑ Evaluate privacy implications of any future on-line, web-based application procedure.
- ❑ Monitor any data collected by or posted on the company's Web sites for privacy concerns.
- ❑ Serve as liaison to government agencies, industry groups and privacy activists in all matters relating to the company's privacy practices.
- ❑ It is the Policy of **STRATEQ HEALTH, INC.** to fully document the assignment of overall security responsibility, and all related activities and efforts, according to our Documentation Policy and HIPAA requirements.

Compliance and Enforcement

All managers and supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **STRATEQ HEALTH, INC.**'s Sanction Policy.