Policy Number: SHI-PP-019
Effective Date: Jan 01, 2020
Last Revised: _____

Information Systems Activity Review Policy

Introduction

STRATEQ HEALTH, INC. has adopted this Information Systems Activity Review 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 Information Systems Activity Reviews 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 information systems activity review, in accordance with the requirements at § 164.308(a)(1).

Policy Statement

- ❑ It is the Policy of **STRATEQ HEALTH, INC.** to regularly review various indicators and records of information system activity, including, but not limited to: audit logs; access reports; and security incident reports.
- ❑ The goal of this Information Systems Activity Review Policy is to prevent, detect, contain, and correct security violations and threats to individually identifiable health information, whether in electronic or any other forms.
- ❑ It is the Policy of **STRATEQ HEALTH, INC.** to fully document all information system activity review activities and efforts.
- ❑ This Information Systems Activity Review Policy shall be implemented and executed in accordance with our risk management policies and procedures.

Procedures

- ❑ Review Alarms settings in each utilized AWS service
- ❑ Review logs in AWS CloudWatch, and each utilized AWS service
- ❑ Review Armor portal and report
- ❑ Review logs in Tenant Management System (TMS)
- ❑ Review logs in Hospital Information System (TMS)

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.