Policy Number: SHI-PP-022
Effective Date: Jan 01, 2020
Last Revised: _____

Access Termination Policy

Introduction

STRATEQ HEALTH, INC. has adopted this Access Termination 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 termination of individual access to individually identifiable health information and Protected Health Information 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 termination of workforce member access to individually identifiable health information and Protected Health Information, in accordance with the requirements at § 164.308(a)(3).
- Prompt and appropriate termination of workforce member access to individually identifiable health information and Protected Health Information can greatly reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- ❑ It is the Policy of **STRATEQ HEALTH, INC.** to terminate any workforce member's access to individually identifiable health information and Protected Health Information when their employment relationship with our organization ends, or when the workforce member has been sanctioned for serious offenses or violations of policy, in accordance with our Sanction Policy.
- ❑ Termination of workforce member access to individually identifiable health information and Protected Health Information must be effected immediately upon the occurrence of a triggering event, such as termination of employment or a positive finding of a serious policy violation or HIPAA offense.
- ❑ In no case shall the termination of access to individually identifiable health information and Protected Health Information be delayed more than 24 hours from the moment of such a triggering event.
- ❑ It is the Policy of **STRATEQ HEALTH, INC.** to fully document all access termination-related activities, in accordance with our Documentation Policy.

Procedures

- ❑ Revoke OpenVPN access
- ❑ Revoke AWS IAM Key
- ❑ Inactivate TMS user access
- ❑ Inactivate Office365 access

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.