Policy Number: SHI-PP-008
Effective Date: Jan 01, 2020
Last Revised: _____

Breach Notification Policy

Introduction

STRATEQ HEALTH, INC. has adopted this Breach Notification 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 Breach Notification 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 concerned with notifications to patients and consumers about breaches of individually identifiable health information, in accordance with the requirements at § 164.400 to § 164.414.
- ❑ Compliance with HIPAA's breach notification requirements is mandatory and failure to comply can bring severe sanctions and penalties.
- ❑ Timely notifications to affected Covered Entities about breaches of individually identifiable health information and Protected Health Information can help reduce or prevent identity theft and fraud.

- ❑ Timely notifications to affected Covered Entities about breaches of individually identifiable health information and Protected Health Information can help protect our business and reputation.

Definitions

As used within the HIPAA Final ("Omnibus") Rule, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.

1. Breach excludes:
    i. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.
    ii. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.
    iii. A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
2. Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
    i. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
    ii. The unauthorized person who used the protected health information or to whom the disclosure was made;
    iii. Whether the protected health information was actually acquired or viewed; and
    iv. The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.

Policy Statement

- ❑ It is the Policy of **STRATEQ HEALTH, INC.** to provide timely notifications to the affected Covered Entity about all breaches of Protected Health Information.
- ❑ **STRATEQ HEALTH, INC.** shall notify the affected Covered Entity when any breach of Protected Health Information is discovered. A breach is treated as "discovered" by **STRATEQ HEALTH, INC.** the first day on which such breach is known or should reasonably have been known to any employee or agent of **STRATEQ HEALTH, INC.**, other than the person who committed the breach.

Procedures

- ❑ Breach Notices must include a brief description of what happened, a description of the types of PHI involved, a brief description of the actions taken in response to the breach, and contact procedures for the Covered Entity to ask questions and obtain further information.
- ❑ Telephone and email shall be the default methods of notification to the Covered Entity.
- ❑ Business Associates (subcontractors) of **STRATEQ HEALTH, INC.** are required to immediately report all breaches, losses, or compromises of individually identifiable health information – whether secured or unsecured – to **STRATEQ HEALTH, INC.**'s designated HIPAA Officer or Privacy Officer; or other responsible party (if no Privacy Official has been designated).
- ❑ Business Associate contracts, whether existing or new, shall have corresponding Breach Notification requirements included in them.
- ❑ Sanctions or re-training shall be applied to all workforce members who caused or created the conditions that allowed the breach to occur, according to **STRATEQ HEALTH, INC.**'s Sanction Policy.
- ❑ All breach-related activities and investigations shall be thoroughly and timely documented in accordance with **STRATEQ HEALTH, INC.**'s Documentation Policy.

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.