

# Policy on Security Incident Procedures

## Introduction

**STRATEQ HEALTH, INC.** has adopted this Policy on Security Incident Procedures 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 responses to Security Incidents involving the breach or compromise of 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 security incident procedures, in accordance with the requirements at § 164.308(a)(6) and at § 164.400 to 164.414.
- Appropriate responses to security incidents may include, but are not limited to:
  - Rapid identification and classification of the severity of security incidents.
  - Determination of the actual risk to individually identifiable health information, and the subject(s) thereof.
  - Repairing, patching, or otherwise correcting the condition or error that created the security incident.

- Retrieving or limiting the dissemination of individually identifiable health information, if possible.
  - Making an *immediate* report of a breach, if required, to the affected Covered Entity who supplied the information to us.
  - Mitigating any harmful effects of the security incident.
  - Fully documenting security incidents, along with their causes and our responses.
  - Expanding our knowledge of security incident prevention, through research, analyses of security incidents, and improved training and awareness programs for workforce members.
- Compliance with HIPAA's data protection requirements is mandatory and failure to comply can bring severe sanctions and penalties.

### **Policy Statement**

- It is the Policy of **STRATEQ HEALTH, INC.** to rapidly identify and appropriately respond to all security incidents, regardless of their severity.
- Responsibility for responding to and managing security incidents shall reside with Privacy Officer.
- The Privacy Officer shall develop specific forms and procedures that shall be implemented in response to security incidents.
- It is the Policy of **STRATEQ HEALTH, INC.** to fully document all security incidents and our responses thereto, in accordance with our Documentation Policy and HIPAA requirements.

### **Procedures**

- Privacy Officer to open a case for the incident.
- Privacy Officer to investigate the incident.
- Privacy Officer to consult legal counsel or management whenever necessary.
- Privacy Officer to inform impacted covered entities as soon as possible.
- Privacy Officer to recommend sanctions to the offender.
- Management to execute the sanctions whenever appropriate.

### **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.