

Encryption and Decryption Policy

Introduction

STRATEQ HEALTH, INC. has adopted this Encryption and Decryption 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 Encryption and Decryption 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 encryption and decryption, in accordance with the requirements at § 164.312(a)(1-2).
- The establishment and implementation of an effective encryption and decryption policy is a crucial element in our overall objective of providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **STRATEQ HEALTH, INC.** to establish and maintain this encryption and decryption policy in full compliance with all the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of this encryption and decryption policy, and any procedures associated with it, shall reside with the CTO, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Specific procedures shall be developed to specify the proper usage and application of encryption and decryption for all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ It is the Policy of **STRATEQ HEALTH, INC.** to fully document all encryption and decryption-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- ❑ All databases with PHI shall be encrypted at rest.
- ❑ All access to StrateqEHR and PHI data shall only access via encrypted tunnel either via site-to-site VPN in hospital or OpenVPN with authorized access ID.
- ❑ All email with PHI content shall be encrypted with Office 365 Message Encryption (OME) service.

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.