Policy Number: SHI-PP-025
Effective Date: Jan 01, 2020
Last Revised: _____

Data Backup Policy

Introduction

STRATEQ HEALTH, INC. has adopted this Data Backup 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 Data Backups 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 data backups, in accordance with the requirements at § 164.308(a)(7) and elsewhere in the Regulations.
- ❑ The ability to create and maintain retrievable, exact copies of individually identifiable health information generally, and Electronic Protected Health Information specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
- ❑ The storage of data backups in a separate location, removed from our normal business operations ("offsite") is an essential element of any successful data backup plan.
- ❑ Timely access to health information is crucial to providing high quality health care, and to our business operations.

- Physicians, healthcare providers and others must have immediate, around-the-clock access to patient information.
- No existing media are absolutely guaranteed to provide long-term storage without loss or corruption of data.
- A number of risks to health information exist, such as power spikes or outages, fire, flood, or other natural disaster, viruses, hackers, and improper acts by employees and others.

Policy Statement

- It is the Policy of **STRATEQ HEALTH, INC.** to create and maintain complete, retrievable, exact backups of all individually identifiable health information generally, and Electronic Protected Health Information specifically, held, processed, or stored in the course of business operations, in full compliance with all the requirements of HIPAA.
- All data backups shall be created and maintained in such manner as to ensure the maximum degree of data integrity, availability, and confidentiality are maintained at all times.

Procedures

- **HISTech Team** is responsible for configuring and monitoring daily backups on **STRATEQ HEALTH, INC.**'s Production network, including shared drives containing application data, patient information, financial data, and crucial system information.
- **STRATEQ HEALTH, INC.** utilizes the Multi AZ feature of AWS RDS to allow database recovery to another AWS Available Zone (AZ) with 15 minutes restore point in Time.
- **STRATEQ HEALTH, INC.** will back up all such data automatically, per **AWS RDS** best practice, at 16:20 GMT-0500.
- **AWS RDS** will validate the backup and AWS CloudWatch will generate daily reports and log and email to Strateq Health's IT Team.
- Any errors will be acted upon immediately. HISTech Team will contact AWS technical support as needed to resolve problems and ensure the validity of backup data.
- The **HISTech Team** is responsible for testing the validity of backup data and the ability to restore data in the event of a RDS system problem, failure, or other disaster regularly to ensure data integrity, availability, and confidentiality.
- All personnel who detect or suspect a data backup problem should immediately report the same to the **HISTech Team**. HISTech Team should follow up immediate notification with a written memorandum that includes the following information:
    - Narrative of the data backup problem.
    - How long the problem has existed.
    - Suggested solutions.

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.