SecureHIT Data Management Plan

Table of Contents

SECUREHIT

DATA MANAGEMENT AND BACKUP POLICY

Table of Contents:

Policy:

SecureHIT establishes and implements procedures to create and maintain retrievable exact copies of electronic protected health information. 164.308(a)(7)(ii)(A). The policy and procedures will assure that complete, accurate, retrievable, and tested back-ups are available for all information systems used by SecureHIT.

SecureHIT creates a retrievable exact copy of electronic protected health information (ePHI) before movement of equipment. SecureHIT maintains a record of movements of hardware and electronic media containing ePHI and any person responsible for the movement of the hardware and electronic media. Therefore SecureHIT utilizes these procedures to track the movement of hardware and electronic media containing ePHI in accordance with the standards set forth in the HIPAA Security Rule.

Data backup and the proper storage of backup media are an important part of the day to day operations of SecureHIT 's information security program. To protect the confidentiality, integrity, and availability of ePHI, the organization completes backups on a frequency that is in accordance with its Risk Analysis to assure that data remains available when it is needed. Established guidelines and defined

standards for accountability of hardware and electronic media containing ePHI further safeguard the confidentiality and security of ePHI.

Responsible for Implementation:

It is the responsibility of the Information Systems Security Officer (ISSO) to implement this policy.

Data custodian – upon direction from the CIO, the Data Custodian will assign responsibility for data backup, recovery, and restoration of all information systems.

Data owner SecureHIT-PRHIE - will determine the appropriate backup strategy based upon business need and is responsible for communication to CIO.

Applicable To:

The IS Department and/or any other department or business associate [or individual, i.e., workforce member] that purchases, moves, maintains, and/or creates equipment or media capable of storing or transmitting ePHI.

*Data backups are generally performed by the IS department in a larger organization. Small organizations should delegate an individual to perform this task.

Key Definitions:

Backup: The process of making an electronic copy of data stored in a computer system. Examples of Back-ups Include:

- Full/Complete Backup - a backup/image of all (selected) data, programs, files on the system.
- Incremental Backup - a backup that only contains the files that have changed since the most recent backup (either full or incremental).
- Snap-shot back-up (image backup) – a process to restore/recover the system at a particular state, at a particular point in time

In the event a system does not allow for an electronic backup, SecureHIT will develop an alternative method to create a copy of the ePHI contained on that system, or complete an analysis delineating alternate solutions for compliance (such as a printed copy).

Data Custodians – persons responsible for keeping data and information organized and secure including rearranging data, renaming documents and other, similar activities but does not personally own or create the data.

Data Owners – persons who have the responsibility and authority to access, create and modify certain data as well as authorize or deny access by others to that data, and is responsible for its confidentiality, integrity and availability.

Electronic Media – means:

- Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;
- Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including paper, facsimile, voice, and telephone are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.[1]

Electronic Protected Health Information (ePHI) - any individually identifiable health information protected (protected health information – PHI) by HIPAA that is transmitted by or stored by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.[2]

Hardware - any physical parts of a computer, as distinguished from the data it contains or operates on, and the software that provides instructions for the hardware to accomplish tasks, i.e., the mechanical, magnetic, electronic, and electrical components making up a computer system.

Off-Site: for the purpose of storage of back up media, off-site is defined as any location separate from the building in which the backup was created. It must be physically separate from the creating site.

1 45 CFR §160.103(a)
2 45 CFR §164.503

The environment for off-site storage must meet appropriate security requirements as well as storage standards established by the manufacturer of the backup media.

Protected Health Information (PHI) - individually identifiable health information that is received, created, maintained or transmitted by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- past, present or future physical or mental health or condition of an individual;
- the provision of health care to an individual;
- past, present, or future payment for the provision of health care to an individual.

Privacy and Security Rules do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.[3]

Recovery Point Objective (RPO) - the age of files that must be recovered from backup storage for normal operations to resume.

Response Time Objective (RTO) - the maximum tolerable time limit within which data must be recovered; target time set for resumption of product, service or activity delivery after an incident.

Procedures:

1. Data Backup

    A. A backup, recovery and testing strategy should be determined based upon the SecureHIT's Risk Analysis strategy

        i. The Information/HIPAA Information Systems Security Officer has oversight responsibility and will ensure that further responsibility is properly assigned for the proper management of data.

        ii. The SecureHIT's ISO is responsible for completing the backups and for ensuring effective training of the workforce members assigned to complete backups, for

3 45 CFR §164.502(f)

management of the backup media and for performing periodic testing of restored media.

iii. SecureHIT will perform a daily backup (or at another prescribed, recurring time period) of all systems that create, receive, maintain, or transmit ePHI. While a vendor may specify or recommend a full back up, an incremental back up, or may not specify, the CIO, will determine the frequency with which back-ups are performed, dependent upon each system.

iv. Data backup systems may be manual or automated.

a. Automated systems electronically capture back up locations, date/time, etc.

b. If the process is manual, documentation of the backup should include:

i) Site/location name

ii) Name of the system

iii) Type of data

iv) Date & time of backup

v) Where backup stored (or to whom it was provided)

vi) Signature of individual that completed the back up

B. The data backup plan requires that all media used for backing up ePHI is stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up [i.e., in a location that protects the backups from loss or environmental damage].

C. If an off-site storage facility or backup service is used, a Business Associate Agreement must be used to obtain satisfactory assurances that the Business Associate will safeguard the ePHI in an appropriate manner.

D. Stored data must be accessible and retrievable at all times.

E. All data backups should be tested and data restored to ensure accuracy.

F. When reusable media such as tapes are used as the back up media refer to the "Media Sanitization and Disposal or Reuse" policy.

G. Data back-ups should be tested and data restored, to assure accuracy. Documentation of backup testing, or restore logs, should be maintained and should capture the date and time

the data was restored. Operational procedures for backup, recovery, and testing should be documented and periodically reviewed.

H. Proper management of situations concerning data back-up/data recovery, such as emergencies or other occurrences, should be addressed in the SecureHIT's Disaster Recovery and Business Continuity Plans.

2. Destruction

SecureHIT will determine a record retention policy and data backup retention schedule. This schedule should include a timeline for the destruction (tapes maintained and destroyed) of storage media.

3. Media Movement

It is not possible or economically practical to control all media that enter and leave an organization. SecureHIT makes all reasonable and appropriate efforts to control media entering and leaving the organization. Workforce members are trained to recognize that media containing ePHI is handled in a manner to protect the confidentiality of the data contained on it. Media that contains ePHI that is no longer useful or useable should be sanitized consistent with the "Media Sanitization and Disposal or Reuse" policy**.**

4. Documentation

All documentation required by this policy will be maintained for a period of six years from the date of creation or the date when it was last in effect, whichever is later.[4]

5. Remote Hosted Systems

Contracts for remote hosted systems must assure that the host complies with this policy.

6. Sanctions

4 45 CFR §164. 105(c)(1-2)

A. Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment.

B. Violation of this policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges.

C. Violation may also result in civil and criminal penalties to SecureHIT as determined by federal and state laws and regulations related to loss of data.

D. Violation may also result in liability to SecureHIT related to loss of data.

Applicable Standards/Regulations:

- 45 CFR 164.308(a)(7)(ii)(A) Data Backup Plan
- 45 CFR 164.310(d)(2)(iii) Accountability
- 45 CFR 164.310(d)(2)(iv) Data Backup and Storage
- 45 CFR 164.308(a)(1)(i)(C) Sanction Policy

Version History:

Original Version: 01/31/2024

Prepared by:	Reviewed by:	Content Changed:
Jose Miranda	SecureHIT	New Document

Janet Ríos Colón

Digitally signed by Janet Ríos Colón
Date: 2024.03.13 12:45:03 -04'00'