HIPAA Security Policy #13

Physical Safeguards
Device and Media Controls

Statement of Policy

The Company is a *Business Associate* under the Health Insurance Portability and Accountability Act (HIPAA) Security Regulations. As such, The Company is required to safeguard electronic protected health information (ePHI) in accordance with the HIPAA Security Rule Regulations as well as The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"). These policies reflect The Company's commitment to complying with such Regulations. The Company will comply with the *Covered Entity's* documented HIPAA policies and procedures unless specifically stated in the below policy.

Purpose of Policy

The purpose of the policy is to define the policy and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility; and the movement ePHI within the facility; and to implement methods to properly dispose of ePHI.

Policy

13 Device and Media Controls

TYPE: Standard
REFERENCE: 45 CFR 164.310(d)(1)
SECURITY REGULATION STANDARDS LANGUAGE:
"Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility."

1. The Company will develop or follow a covered entity's policies and procedures that govern receipt, removal, movement and disposal of hardware and electronic media containing ePHI within the facility. The policies and procedures will address device and media controls relating to:

    i. Disposal

    ii. Media Re-use

    iii. Accountability

    iv. Data Backup and Storage

13.1 Disposal

IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 64.310(d)(2)(i)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."

1. The Company must take reasonable and appropriate steps to dispose of portable devices and media that contain ePHI. Removal steps must ensure that ePHI is properly copied off of the device and that destruction of ePHI prevents unauthorized access to the ePHI.

2. The Media Disposal procedure will apply to all systems that contain ePHI that The Company has operational control of and are not covered under the covered entity's Media Disposal procedure.

Procedure

1. Prior to destroying or disposing of any portable device or media, care must be taken to ensure that the device or media does not contain ePHI.

2. If the portable device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to disposal.

3. If the portable device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. A typical reformat is not sufficient as it does not overwrite the data. Note that a data destruction tool which adheres to the Department of Defense (DoD 5220.22-M) standard is recommended to properly destroy ePHI.

3. HIPAA Security Officer or delegate will notify the Information Technology (IT) department/company/individual of equipment that needs to be disposed of.

4. HIPAA Security Officer or delegate will determine data sensitivity of data to be disposed of. (See Data Classification Table below)

5. IT will assess the condition of the equipment, they will:
    a. IT will track the disposal of the device (type of hardware, serial number, etc). See Appendix A: Media Disposal Log
    b. IT will run approved wiping software on all devices to make sure all patient information is removed from the device. This may include physical destruction (See Methods of Destruction below)
    c. IT will verify the hardware's data has been removed
    d. IT will dispose of the hardware

6. HIPAA Security Officer or delegate / IT will document the destruction of the asset and keep a record. See Appendix C: Media Disposal Log

7. If taken to outside facility - The media shall be taken to an approved, certified facility for erasure or destruction. A letter of certification regarding date and time of erasure/destruction shall be obtained

Data Classification Table:

1. **Low (Unclassified)** - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
    - Basic operating system, personal files,
2. **Medium (Sensitive)** - Erase the data using any means such as reformatting or degaussing.
    - Business related information that does not contain patient information (ePHI).
3. **High (Confidential)** - The data must be erased using an approved technology to make sure it is not readable using special technology techniques. (See method of destruction below)
    - Media contains patient information (ePHI).

Examples of hardware devices include:

- Workstation
- Laptop
- Tablet (iPad/Android)
- Smartphones
- Server hard drives
- Memory stick (USB drives)
- CD ROM disk / DVD ROM
- Storage / Backup tape(s)
- Hard drives
- Copiers / Scanners / Fax machines
- X-Rays / Ultrasound / Diagnostic Machines
- Any other hardware that contains ePHI

Methods of Destruction Table:

Clear	One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. A data destruction tool which adheres to the Department of Defense (DoD 5220.22-M) standard is recommended to properly destroy ePHI. Overwriting cannot be used for media that are damaged or not rewriteable.)
Purge	Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.
Destroy	There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack. • Disintegration, Pulverization, Melting, and Incineration. These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • Shredding. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm).

13.2 Media Re-use

IMPLEMENTATION TYPE: Required
REFERENCE: 45 CFR 64.310(d)(2)(ii)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use."

1. The Company must take reasonable and appropriate steps to ensure that portable device and media do not contain ePHI prior to re-use the device or media. If the device or media does contain ePHI then steps must be taken to ensure that the ePHI is properly destroyed prior to re-use of the device or media.

2. The Media Re-use procedure will apply to all systems that contain ePHI that The Company has operational control of and are not covered under the covered entity's Media Re-use procedure.

Procedure

1. Prior to making a portable device or media available for reuse, care must be taken to ensure that the device or media does not contain ePHI.

2. If the device or media contains the only copy of ePHI that is required or needed, a retrievable copy of the ePHI must be made prior to reuse.

3. If the portable device or media contains ePHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to reuse. A typical reformat is not sufficient as it does not overwrite the data. Note that a data destruction tool which adheres to the Department of Defense (DoD 5220.22-M) standard is recommended to properly destroy ePHI

4. The use of a data destruction tool before reuse is not required if the media is used for system or data backup, as long as the media is stored and transported in a secured environment.

13.3 Accountability

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 64.310(d)(2)(iii)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Maintain a record of the movements of hardware and electronic media and any person responsible therefore."

1. When using portable devices or media to transport ePHI, a procedure must be developed to track and maintain records of the movement of such devices and the media and the parties responsible for the device and media during its movement.

2. The Media Accountability procedure will apply to all systems that contain ePHI that The Company has operational control of and are not covered under the covered entity's Media Accountability procedure.

Procedure

1. A log should be maintained of any hardware containing ePHI that has been received into or removed from The Company's facilities. The log should note the workforce member receiving or removing the equipment, the date of receipt or removal, the

person approving the receipt or removal, and the date the hardware was returned. (See Appendix A Receipt of Hardware or Electronic Media Containing ePHI Log and Appendix B Removal of Hardware or Electronic Media Containing ePHI Log).

13.4 Data Backup and Storage

IMPLEMENTATION TYPE: Addressable
REFERENCE: 45 CFR 64.310(d)(2)(iv)
SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:
"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."

1. Before moving any systems that contain ePHI, a procedure must be developed to ensure that the ePHI is properly backed up and secured prior to moving.

2. The Media Data Backup procedure will apply to all systems that contain ePHI that The Company has operational control of and are not covered under the covered entity's Media Data Backup procedure.

Procedure

1. If a system contains ePHI, all files containing ePHI must be backed up to a computer, tape, USB drive, CD-ROM, disk, or other storage media before equipment is moved within or outside of The Company's facilities.

2. The backed-up data should be stored in a secure area until it is placed on different equipment or restored to the original equipment from which it was removed.

Appendix A Receipt of Hardware or Electronic Media Containing ePHI Log

Item #		Patient Name(s)	Description of Hardware or Electronic Media	Reason for Receipt	Date of Return	Returned To:
	Date Received	Received From	Received By (Name)	Received By (Signature)	Returned By (Name)	Returned By (Signature)

Appendix B Removal of Hardware or Electronic Media Containing ePHI Log

Item #		Reason for Removal	Approved By (Name)	Removed By (Name)	Returned By (Name)	Date of Return
	Date Removed	Description of Hardware or Electronic Media	Approved By (Signature)	Removed By (Signature)	Returned By (Signature)	Returned To:

Appendix C: Media Disposal Log

The below data was disposed / destroyed as required in **HIPAA Security Policy #13 – Device and Media Control.**

Date of Destruction:

Authorized By: Click here to enter text.

Description of Information Disposed of or Destroyed (include Manufacturer/Model/Serial Number/etc):

Click here to enter text.

Backup of Protected Health Information (PHI)? Required if PHI is the only copy.

☐ Yes

☐ No

If Yes, List Backup Location: Click here to enter text.

Method of Destruction:

☐ **Clear** (One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable.)

☐ **Purge** (Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes.

☐ **Destroy** (Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting. If destruction is decided upon due to the high security categorization of the information or due to environmental factors, any residual medium should be able to withstand a laboratory attack.

Disintegration, Incineration, Pulverization, and Melting. These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal

destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.

Shredding. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality level that the information cannot be reconstructed.

Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and magneto-optic (MO) disks must be destroyed by pulverizing, crosscut shredding or burning)

Destruction Method Used:

Click here to enter text.

Final Disposition of Media:

☐ Disposed

☐ Reused Internally

☐ Reused Externally (sold / donated / etc.)

☐ Returned to Manufacturer / Leasing Company / Vendor / etc.

☐ Other: Click here to enter text.

Save this log and retain indefinitely. Upload to the Compliance Portal.