**PS – D (1 & 2) Device and Media Controls**

***Purpose***

To 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.

**Guidance**

Covered entities must implement documented policies and procedures to govern the receipt and removal of electronic hardware that may contain ePHI.

**Disposal**

Implementation: Ensure that ePHI on hardware and electronic media, including copiers, faxes, printers, etc., is unusable and/or inaccessible prior to disposal, including disposal by a Business Associate.164.310(d)(2)(i)

* When portable media is discarded, it must either be overwritten in accordance with National Institute of Standards and Technology (NIST) [guidelines](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf), or physically destroyed, eliminating all possibility that any ePHI contents could be read.
* When a system is recycled, transferred to another user not authorized for the data, or discarded, all storage devices or all ePHI records must be overwritten in accordance with NIST guidelines (link above), or physically destroyed, rendering all ePHI records unreadable.

**Media Re-use**

Implementation: Create procedures for the removal of electronic protected health information from electronic media before the media is made available for re-use. 164.310(d)(2)(ii)

* Ensure that ePHI on hardware and electronic media is unusable and/or inaccessible prior to re-use.
* When a system is recycled or transferred to another user not authorized for the data, or otherwise re-used outside of a HIPAA-compliant environment, all storage devices or all ePHI records must be overwritten in accordance with National Institute of Standards and Technology (NIST) guidelines, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>, rendering all ePHI records unreadable.

**Accountability**

Implementation: Maintain a record of the movements of hardware and electronic media and any person responsible therefore. 164.310(d)(2)(iii)

* The responsible HIPAA entity must maintain a record of the movements of, and person(s) responsible for, hardware and electronic media containing ePHI.
	+ Identify all types of hardware and electronic media that must be tracked.
	+ Special attention must be paid to portable devices and removable media. These devices should not ordinarily contain ePHI. However if they do, they must be individually identified in the tracking system. Their use must be consistent with the individual’s identified role, such as according to a role-based matrix.
	+ This inventory should be physically confirmed at least annually.
	+ Tracking system must include a mechanism for documenting the initial assignment of responsibility for devices that contain ePHI, as well as the transfer of authority for these devices.
* Transport of archival media between the origination point and remote storage location must use a secure method to avoid unauthorized access to the archival media.
* Loss or theft of electronic equipment or media containing ePHI must immediately be reported according to the Information Security Office [incident response procedures](http://louisville.edu/security/incident-reporting-and-response).

**Data Backup and Storage**

Implementation: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment. 164.310(d)(2)(iv)

Create a retrievable, exact copy of original sources of essential ePHI before moving equipment containing them.

* Establish a process for documenting or verifying its creation.
* Retrievable, exact copies of ePHI must be protected in accordance with these Standards.