4.13. Device and Media Controls (§ 164.310(d)(1))

HIPAA Standard: *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.*

Key Activities	Description	Sample Questions
1. Implement Methods for Final Disposal of EPHI **Implementation Specification (Required)**	• *Implement policies and procedures to address the final disposition of EPHI and/or the hardware or electronic media on which it is stored.* • Determine and document the appropriate methods to dispose of hardware, software, and the data itself. • Assure that EPHI is properly destroyed and cannot be recreated.	• What data is maintained by the organization, and where? • Is data on removable, reusable media such as tapes and CDs? • Is there a process for destroying data on hard drives and file servers? • What are the options for disposing of data on hardware? What are the costs?
2. Develop and Implement Procedures for Reuse of Electronic Media **Implementation Specification (Required)**	• *Implement procedures for removal of EPHI from electronic media before the media are made available for reuse.* • Ensure that EPHI previously stored on electronic media cannot be accessed and reused. • Identify removable media and their use. • Ensure that EPHI is removed from reusable media before they are used to record new information.	• Do policies and procedures already exist regarding reuse of electronic media (hardware and software)? • Is one individual and/or department responsible for coordinating the disposal of data and the reuse of the hardware and software? • Are employees appropriately trained on security and risks to EPHI when reusing software and hardware?[75]
3. Maintain Accountability for Hardware and Electronic Media **Implementation Specification (Addressable)**	• *Maintain a record of the movements of hardware and electronic media and any person responsible therefore.* • Ensure that EPHI is not inadvertently released or shared with any unauthorized party. • Ensure that an individual is responsible for, and records the receipt and removal of, hardware and software with EPHI.	• Where is data stored (what type of media)? • What procedures already exist regarding tracking of hardware and software within the company? • If workforce members are allowed to remove electronic media that contain or may be used to access EPHI, do procedures exist to track the media externally? • Who is responsible for maintaining records of hardware and software?
4. Develop Data Backup and Storage Procedures **Implementation Specification (Addressable)**	• *Create a retrievable exact copy of EPHI, when needed, before movement of equipment.* • Ensure that an exact retrievable copy of the data is retained and protected to protect the integrity of EPHI during equipment relocation.	• Are backup files maintained offsite to assure data availability in the event data is lost while transporting or moving electronic media containing EPHI? • If data were to be unavailable while media are transported or moved for a period of time, what would the business impact be?

[75] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*