TMA Privacy Office Information Paper

Device and Media Controls

HIPAA Security◆ November 2003

Standard Requirement

Covered entities must implement device and media controls as a part of their physical safeguards. The HIPAA Security Rule defines those as "policies and procedures that govern the receipt and removal of hardware and electronic media that contain protected health information into and out of a facility, and the movement of these items within the facility." The standard requires covered entities to develop policies and procedures that will guard the electronic protected health information (EPHI) on both hardware and movable media. DHHS has noted that "device" and "media" are to be interpreted broadly. (Final Rule, p.8354 and p. 8374) Media includes drives (permanent and removable), diskettes, compact discs, tapes and any other device that is capable of storing electronic information. The movement of these devices must be protected within a facility and when they enter or leave a facility.

Implementation Specifications

Four implementation specifications expand on aspects of media controls; the first two are required, the last two addressable:

- disposal,
- media re-use,
- accountability, and
- data backup and storage.

The first required implementation specification, disposal, mandates implementation of "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." Each covered entity must implement safeguards for the disposal of EPHI, hardware and electronic media. As covered entities replace and update hardware and other media, EPHI often remains on hard drives and other media. This implementation specification requires policies and procedures for preventing EPHI from being disclosed while disposing of EPHI or electronic media and devices used to store EPHI. Policies and procedures should include approved methods of disposal such as use of commercial or public disposal services, sale or donation of electronic devices and the process for ensuring that EPHI processed by or stored on the hardware and electronic media is no longer accessible.

The second required implementation specification, media re-use, is closely related: policies and procedures for "removal of electronic protected health information from electronic media "before the media are made available for re-use." Each covered entity must remove EPHI before electronic media is re-used. Electronic devices and media are often reused in the normal course of business. For example new employees often receive workstations used by previous employees. This implementation specification requires that the covered entity establish procedures for authorizing media for re-use and for removing EPHI before re-use depending on the environment and the sensitivity of the information. Although some overlap exists with the disposal implementation specification, this implementation specification emphasizes all possible re-uses of the media or electronic devices by personnel and systems inside and outside of the covered entity. Disposal concerns discarding of the media, which might include reuse by persons

Device and Media Controls

or systems outside the organization. A covered entity's risk management plan should describe and justify procedures for implementing the media re-use policies.

The third implementation specification, accountability, covers maintenance of "a record of the movements of hardware and electronic media and any person responsible therefore." Because this requirement is "addressable", compliance depends on the outcome of a covered entity's risk assessment. Staff of covered entities often process and store protected health information on highly portable, electronic media thus creating a potential for theft or loss. A covered entity's policies must require evaluating the need for procedures to mitigate this threat as part of its information security risk assessment. A covered entity should describe and justify as part of its risk management plan procedures for safely managing electronic devices and media, including records of who has the devices or media, when they had possession, and where they kept the devices or media from the time of original receipt to time of final disposal or transfer to another entity. The mechanism used for recording this information may be manual or automated.

The last implementation specification, data backup and storage, addresses creation of "a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment." (A broader requirement for data backup and disaster recovery is part of the contingency plan standard, as well as implicit in the data integrity standard.) Because this implementation specification is "addressable", compliance depends on the outcome of a covered entity's risk assessment. Covered entities must perform data backup as part of the contingency plan requirement. As part of the device and media control requirement in physical safeguards, this addressable implementation specification stipulates controls governing the movement and availability of backups. Electronically stored information can be lost, damaged, or destroyed if stored improperly or when equipment is moved. A covered entity should address threats to the confidentiality, integrity and availability of EPHI on equipment being moved and during storage in its information security risk assessment. The risk management plan should describe and justify its approach to issues such as secure movement of equipment, media shelf life and retention periods, the conditions of short and long-term storage locations, and physical protection measures for media repositories. Covered entities should document policies as part of its risk management plan and include the procedures in the standard operating procedures of its contingency plan.

See also:
45 CFR 164.310(d)(1)

Federal and DoD regulations that support this standard
DoD 8510.1-M
DoDI 8500.2