Health Information Compliance Alert

Sample Policy: Prevent Media Disposal Mishaps With This Policy

Train staffers on the appropriate steps to take when their hardware's time is up.

A sound policy is the best place to start when planning to destroy or re-use hardware in your facility.

Use this sample, contributed by **William Hubbartt**, a health care consultant with Hubbartt & Associates in St. Charles, IL, as a guide to help you create the right policy and procedures for your organization.

Media Disposal and Re-use

The Security Officer is responsible for defining and implementing disposal or repurposing guidelines for media and devices (including diskettes, CDs, cartridges, portable devices and all other software or hardware) that contain electronic PHI (e-PHI) as required by HIPAA.

The Security Officer must oversee disposal of media and devices as follows:

1. The Security Officer and the Administrative Director will determine which media and devices are subject to disposal.

2. Workforce members must turn all media and devices over to the department supervisor so that they can be prepared for disposal.

3. The department supervisor must determine what data (i.e., non-sensitive information, proprietary data or e-PHI) is contained on the media or device and evaluate whether such data shall be retained or subject to disposal.

4. The supervisor will designate a workforce member or team to transfer or copy any data that must be retained.

5. The Security Officer shall oversee or delegate the final destruction of the media or device. This actionshall be documented by the individual(s) performing such task.

The Security Officer must oversee repurposing of media or devices as follows:

1. The Security Officer and the Administrative Director should decide which hardware device(s) and/or software can be repurposed.

2. The employee currently using the media or device and the department supervisor must work together to determine what data (i.e., non-sensitive information, proprietary data or e-PHI) is contained on the media or device and evaluate whether such data shall be retained or erased.

3. The employee currently using the media or device will be responsible for transferring or copying any data that must be retained.

4. The department supervisor shall send the media or device to the Information Services (IS) department so that it can be erased, re-formatted or otherwise sanitized. This action shall be documented by the individual(s) performing such task.

5. The sanitized media or device will be turned over to the correct department or entity for re-distribution. The Security Officer must maintain a record of how all media and devices move through the organization, from purchase through disposal. The record must include the names of those responsible for the media and devices within the entity.

Codify
BY AAPC

Reprinted with permission from "The HIPAA Security Rule -- A Guide for Employers & Health Care Providers."