



Title: Disposal of Material containing Protected Health Information and other Confidential Information.

Issue:

Proper disposition of Protected Health Information (PHI) and other confidential information on paper documents and or portable electronic media (e.g., floppy disks, CD....)

Facts:

- HIPAA requires that each patient's confidentiality be protected.
- HIPAA requires media (whether paper or electronic) that contains PHI be properly disposed when no longer needed.
- HCHD confidential information must be properly disposed when no longer needed.
- Proper disposal requires that paper be shredded; electronic media be deleted, erased or reformatted; and other readable forms of media be defaced or rendered unusable.

Elaboration:

Background

The Harris County Hospital District, as a HIPAA defined covered entity is responsible for ensuring the privacy of our patients and maintaining confidentiality of their Protected Health Information (PHI) and their Designated Record Set (DRS) that is comprised of medical and billing files. Prior to HIPAA, Hospital District facilities and departments utilized various methods of disposing of information, typically with the use of small paper shredders. During the HIPAA Assessment, a number of solutions to dispose of PHI and confidential documents were evaluated. The final decision was to pursue an onsite system of destroying documents.

The Hospital District purchased and installed a commercial grade shredder and paper bailer. The shredder allows the Hospital District to convert those documents, containing either PHI or other confidential information, into small strips of paper or "confetti."

Guideline

All departments, facilities and organizations of the Harris County Hospital District are required to identify those documents, used in the course of their job responsibilities, that contain PHI and dispose of them into containers designated for recycled paper. PHI is actually identifiers and/or medical/clinical information that is either included in the content of information or used in a header/footer as information to "identify an individual; or their relative(s), employer or other household member(s)." The definition of PHI and a list of the identifiers are listed below:



Protected health information (PHI) is individually identifiable patient health information in any form, including demographic information, that is created or received by a healthcare provider, and relates to the patient's healthcare condition, provision of healthcare, or payment for the provision of healthcare. The following is a list of the PHI identifiers and any document containing any of the following must be protected and should be disposed of in a container designated for recycled paper.

- 1.) Names,
- 2.) Geographic subdivisions smaller than a state (e.g., city, town, precinct, zip, etc...),
- 3.) All elements of dates (except year) relating to an individual including the following: a) birth, b) admission, c) discharge, d) death, e) ages over 89 years,
- 4.) Telephone numbers,
- 5.) Fax numbers,
- 6.) E-mail addresses,
- 7.) Social security numbers,
- 8.) Medical record numbers,
- 9.) Health plan beneficiary numbers,
- 10.) Account numbers,
- 11.) Certificate /license numbers,
- 12.) Vehicle identifiers, serial numbers and license plates numbers,
- 13.) Device identifiers and serial numbers,
- 14.) Web Universal Resource Locators (URL),
- 15.) Internet Protocol (IP) address numbers,
- 16.) Biometric identifiers, including finger and voice prints,
- 17.) Full face photographic images,
- 18.) Any other unique identifying number, characteristic or code unless permitted.

All protected health information must be removed from all computer equipment before leaving District control or being reused. The method used must comply with U.S. Department of Defense (DOD) standards, and may be degaussed (erasing information from storage media by passing it through a magnetic field) or wiped clean with software programs that adhere to that standard. All removable media (magnetic or optical) must be forwarded to Field Services for disposal and requires degaussing or use of other industry standard methods to render the data unusable prior to disposal. Reports of all electronic information disposals must be forwarded to the HIPAA Security Officer, who will maintain a record of all actions performed and periodically audit the procedures.

References:

- 45 CFR §164.530 (c) Safeguards
- 45 CFR § 164.514 (a) de-identification of PHI
- HIPAA Policy 3.11 (CFR §164.502)