TMA Privacy and Civil Liberties Office Information Paper

BEST PRACTICES FOR DISPOSING PHI

HIPAA Privacy ◆ September 2011

I. Supporting Regulations for Disposing PHI

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule establishes the requirement for covered entities to have appropriate administrative, technical, and physical safeguards in place to protect the privacy of protected health information (PHI), including the disposal of such information. See 45 CFR 164.530(c).

B. The Department of Defense Health Information Privacy Regulation (DoD 6025.18-R) implements the above part of the HIPAA Privacy Rule within the Military Health System (MHS). See C14.3.

C. The HIPAA Security Rule establishes the requirements for covered entities to implement policies and procedures regarding the disposal of electronic PHI. See 45 CFR 164.310(d)(2).

D. The DoD Health Information Security Regulation (DoD 8580.02-R) implements the above part of the HIPAA Security Rule within the MHS. See C3.5.3.

II. Definitions Associated with Disposing PHI

A. Administrative Safeguards: Administrative actions, and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to safeguard electronic PHI and to manage the conduct of an organization's workforce in relation to the protection of that information.

B. Business Associate: A person or entity that performs or assists in the performance of a function or activity (legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services) involving the use or disclosure of PHI on behalf of, or to provide services to, an organization, as defined in DoD 6025.18-R (Reference (f)).

C. Covered Entity: A health plan or a healthcare provider within the MHS that transmits any health information in electronic form to carry out financial or administrative activities related to healthcare.

D. Disclosure: The release, transfer, provision of access to, or revealing in any other manner of PHI outside the entity holding the information.

E. Electronic Media: Includes memory devices in computers (e.g., hard disks, memory chips) and any removable or transportable digital memory medium, such as magnetic tape or disks, optical disks, digital memory cards, or transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet, the extranet, leased lines, dial-up lines, private networks, and the physical movement of removable or transportable electronic storage media. Traditional paper-to-paper facsimile is not included; however, electronic data transmitted using a computer-based facsimile program is included.

F. Military Health System (MHS): All DoD health plans and all DoD healthcare providers that are, in the case of institutional providers, organized under the management authority of, or in the case of covered individual providers, assigned to or employed by TMA, the Army, the Navy, or the Air Force.

G. Physical Safeguards: Physical measures, policies, and procedures to protect an organization's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

H. Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained by electronic or any other form or medium, except as otherwise contained in employment records held by a covered entity in its role as an employer.

I. Technical Safeguards: The technology and the policy and procedures for its use that safeguard electronic PHI and control access to it.

J. Use: With respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

III. Suggested Best Practices for Disposing PHI

A. The HIPAA Privacy and Security Rules require covered entities to reasonably safeguard PHI from any intentional or unintentional use or disclosure. Therefore, covered entities should safeguard against disposing trash containing PHI in locations, such as dumpsters, that are accessible by the public or other unauthorized individuals.

B. The HIPAA Privacy and Security Rules do not specify a certain method to dispose of trash containing PHI, however:

1. Covered entities should review their particular environment to develop and implement reasonable policies and procedures for the disposal of trash from all secure and non-secure spaces. This is a precaution against unintentional disclosure of any PHI that may have been thrown in the trash by a patient.
2. Covered entities should assess potential privacy risks regarding the form, type, and amount of trash containing PHI to be disposed.
    a. For example, the disposal of more sensitive PHI – Social Security Numbers, diagnosis, financial account numbers, or treatment information - may require more protections.
3. Examples of proper disposal methods of PHI may include, but are not limited to:
    a. Paper:
        i. Shredding,
        ii. Burning,

iii. Pulping,

iv. Pulverizing, or

v. Otherwise rendered unreadable, and unable to be reconstructed.

b. Electronic:

i. Clearing (using software or hardware products to overwrite media with non-sensitive data),

ii. Purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or

iii. Destroying (disintegration, pulverization, melting, incinerating, or shredding).

b. Other:

i. Maintaining labeled prescription bottles and similar forms of PHI in a secure area in opaque bags, and

ii. Using a business associate disposal vendor to remove and shred or otherwise destroy the PHI.

C. Covered entities are responsible for ensuring that their workforce members, including volunteers, are properly trained on the policies and procedures for disposal of PHI.