Information Access Management

HIPAA Security Information Paper ♦ March 2010

TMA Privacy Office Information Paper

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs

PURPOSE:

The purpose of this paper is to elaborate on the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Security Rule "Information Access Management" requirements as specified by DoD Regulation 8580.02-R, "Health Information Security Regulation", (reference (a)). The following policy outlines the procedures which are required.

BACKGROUND:

The HIPAA Security Rule requires covered entities, i.e., MHS, to implement an information access management plan as part of their administrative safeguards. This plan should include policies and procedures for authorizing access to electronic protected health information (ePHI). It also must determine who may access what types of health information. While this access is not based on worker roles, this rule does require differentiating information access given to different categories of workers. This differentiation depends on the covered entity's risk analysis, size, structure and business needs. This means that a covered entity would first establish a set of policies that lists and describes the different categories of workers; second, determine the types of information needed by each of those categories of workers; and third, establish the permitted uses (read, write, amend) of each type of information for each category. Each worker should only have access to the minimum amount of information needed to achieve the purpose of its use. Included in this plan should be policies and procedures that describe how each worker is given access to information, determine who has the authority to assign categories and the level of access given to that category, and finally, determine the process for setting up accounts, including how to make changes to existing accounts. A corresponding set of policies and procedures should include periodic reviews of the accounts to ensure that they are current and accurate.

POLICY:

Covered entities should implement an information access management plan as part of their administrative safeguards. This plan shall include policies and procedures for authorizing access to ePHI.

Access: Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of reference (b) and (c).

TMA Privacy Office 5111 Leesburg Pike, Suite 810 Falls Church, VA 22041

Information Access Management

Differentiation: Differentiate information access provided to different categories of workers as based on the organization's risk analysis, size, structure, individual access requirements and business needs.

- Establish a policy that lists and describes the different categories of workers.
- Determine the types of information needed by each of those categories of workers.
- Establish the permitted uses (read, write, amend, delete) of each type of information for each category. Only grant each worker access to the minimum amount of information needed according to their access requirements and/or to achieve the purpose of its use.

Management: Establish policies and procedures for workforce configuration management that describe how the workforce is given access to information and determine the process for implementing workforce accounts, including how to make modification to permission to existing accounts. Include periodic reviews for requesting, establishing, issuing and closing workforce accounts to ensure that they are current and accurate.

Access Authorization: Implement policies and procedures for granting an individual access to ePHI through multiple venues to include: access to a workstation, transaction, program, process, or other mechanism. Include clear delineation on the required authorizations and clearances needed before an account can be established.

Access Establishment and Modification: Based upon the organization's access authorization policies, implement additional policies and procedures that establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Integration: The policies and procedures listed in sections C2.5.4. and C2.5.5. of reference (a) are very similar to those of the Workforce Security section (C2.4., reference (a)). This redundancy reflects the importance of a formal configuration management process and

Information Access Management

documented policies and procedures that define the level of access for personnel authorized access to ePHI, including how the access is granted, modified, and terminated.

REFERENCES:

(a) DoD Regulation 8580.02-R, "Health Information Security Regulation", July 12, 2007

(b) DoD Regulation 6025.18-R, "DoD Health Information Privacy Regulation", January 2003

(c) Sections 3541 - 3544 of Title 44, United States Code, "Federal Information Security Management Act of 2002"