



TMA Privacy Office Information Paper

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



Workforce Security

HIPAA Security Information Paper ♦ March 2010

PURPOSE:

The purpose of this paper is to elaborate on the Health Insurance Portability and Accountability Act (HIPAA) of 1996 Security Rule “Workforce Security” 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 a workforce security program. Workforce Security is defined as the implementation of policies and procedures to ensure that all members of the workforce have appropriate access to electronic protected health information (ePHI). The term “workforce” includes all personnel, even those that are not directly involved in patient care, like cleaning personnel or the occasional maintenance or repair contractor. Other examples include full-time employees and part-time employees, contract personnel, volunteers, students and trainees.

POLICY:

Covered entities implement policies and procedures to ensure that all members of the workforce have appropriate access to ePHI.

Access: Implement policies and procedures to ensure that all members of the workforce have appropriate access to ePHI, as provided under reference (a). Prevent those workforce members who do not have authorized access, either physical or electronic, from obtaining contact with ePHI.

Workforce: The term “workforce” includes military and civilian full-time and part-time employees, contract personnel, volunteers, students, and trainees. Ensure that individuals such as cleaning personnel and facility maintenance or repair contractors are considered and addressed in policies and procedures.

Authorization and/or Supervision: Implement procedures for the authorization and/or supervision of workforce members. A workforce member working with or in locations accessible to ePHI must either be authorized to be there, supervised while there, or both. The organization may employ various procedures across different types of workers depending on the results of the risk analysis, cost, and the organization’s resources and business processes as long as these procedures are documented.



TMA Privacy Office Information Paper

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



Workforce Security

HIPAA Security Information Paper ♦ March 2010

Workforce Clearance Procedures: Implement procedures to determine the appropriate access of workforce members to ePHI.

- Implement personnel security background investigation procedures for access to ePHI that determine a person's trustworthiness in accordance with DoD 5200.2-R (reference (b)). A workforce member's access to ePHI is dependent on assessments of their job responsibilities including the amount and type of supervision.
- Implement a screening process for each job position or role and document the procedures to be followed in conducting that check. While some roles may require job references or a National Agency Check with Local Agency and Credit Check (NACLIC), others may not require any process beyond an interview.

Termination Procedures: Implement procedures for terminating access to ePHI when the employment of a workforce member ends or as required by the organization's workforce clearance and access procedures required by references (a). Termination procedures must focus on two common threats: (1) continued access to information by terminated workforce personnel and (2) continued access to information by those who are still part of the workforce but whose access is no longer appropriate. Workforce status ends for many different reasons, such as retirement, change of jobs, or unsatisfactory performance, and each reason potentially poses different threats to information assets. Depending upon its risk assessment, an organization may require different procedures for terminating a former employee's access to information versus changing the access permissions for a current employee.

REFERENCES:

- (a) DoD 8580.02-R, "Health Information Security Regulation", July 12, 2007
- (b) DoD 5200.2-R, Change 3, "Personnel Security Program", February 23, 1996