TMA Privacy and
Civil Liberties Office
Information Paper

ROLE-BASED ACCESS

HIPAA Privacy ◆ February 2012

I. Supporting Policies for Role-Based Access

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule establishes requirements regarding minimum necessary uses of protected health information (PHI). See 45 CFR 164.514(d)(2).

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 Paragraph C8.2.3.

C. The HIPAA Security Rule establishes requirements regarding implementing policies and procedures for authorizing access to PHI. See 45 CFR 164.308(a) (4)(i).

D. The DoD Health Information Security Regulation (DoD 8580.02-R) implements the above part of the HIPAA Security Rule within the MHS. See Paragraph C2.5.

II. Definitions Associated with Role-Based Access

A. 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.

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

C. 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.

D. Minimum Necessary: The minimum amount of PHI that is reasonably needed to achieve the purpose of a requested use, disclosure or request for PHI.

E. 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.

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

III. Guidance Regarding Role-Based Access

A. Covered entities should make reasonable efforts to limit access to PHI to workforce member that require access based on their roles.

B. Covered entities should develop and implement role-based access policies and procedures that authorize workforce members to access PHI for authorized purposes, as appropriate. These policies and procedures should:

   1. Identify the categories of workforce members who need access to PHI to perform their assigned tasks.
   2. Specify the type of PHI needed by each category of workforce members and any conditions appropriate to such access.
   3. Establish the permitted uses of each type of PHI for each workforce member category.
   4. Specify that each worker will be granted access to the minimum amount of PHI necessary according to their access requirements and/or to achieve the purpose of its use.

C. A covered entity's system administrator should establish the appropriate accounts to ensure that an individual workforce member's access is only granted to the appropriate level in accordance with the covered entity's policies and procedures.

   1. Requests for additional access should not be granted unless the individual's responsibilities change such that he or she is in a different workforce category necessitating the increased access.
   2. Procedures should be established to periodically monitor and validate access requirements. Ensure user access is promptly terminated or downgraded as necessary to align with the individual's workforce responsibilities.

D. Covered entities are responsible for ensuring that their workforce members are properly trained on the policies and procedures for accessing and safeguarding of PHI prior to granting access.

E. Covered entities should establish procedures to notify system administrators of personnel changes including internal transfers and job requirements changes, in order to assign and delete electronic medical record access as appropriate.

F. Covered entities should establish comprehensive policy and procedures for timely notification from departments to system administrators of personnel changes (for example, external transfers, separations and deployments), including out-processing checklists.