TMA Privacy Office Information Paper

Security Evaluation

HIPAA Security ♦ September 2012

I. Supporting Regulations for this Information Paper

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (45 CFR 164.308(a)(8)) requires covered entities to perform a periodic technical and non-technical security evaluation.

B. The Department of Defense Health Information Security Regulation (DoD 8580.02-R, C2.9. (C2.9.1. - C2.9.3.)) implements the above part of the HIPAA Security Rule within the Military Health System (MHS).

II. Guidance For Security Evaluation

A. General Requirement: The HIPAA Security Rule requires covered entities to have a periodic technical and non-technical security evaluation that establishes the extent to which a covered entity's security policies and procedures meet the requirements of the HIPAA Security Rule. Examples of such requirements includes, but is not limited to, policies and procedures required within DoD 8580.02-R on access controls, logging of movement of media with PHI, or policies and procedure for transmission security. According to the Security Rule, this evaluation is "based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information (ePHI)." This means that covered entities must assess how changes in the environment (e.g. security-related regulations and laws, new threats) and in their operations (e.g. changing mission, business practices, upgraded or new technology) will affect their compliance. The requirement for both "technical and non-technical" assessment indicates that the evaluation must include all organizational safeguards and systems, as well as a review of information systems. These security evaluations can either be performed by a covered entity's own workforce members or an outside organization, which would be acting as a business associate. This decision is left up to the covered entity.

B. Implementation Specification: Covered entities are required to perform a periodic technical and non-technical security evaluation that establishes the extent to which a covered entity's security policies and procedures meet the following requirements:

1. Perform an annual (or more frequent) technical and non-technical evaluation of the security program based on DoD 8580.02-R and in response to environmental or operational changes affecting the security of ePHI. Establish the extent to which the organization's security policies and procedures meet the requirements of DoD 8580.02-R.

2. Assess how changes in the environment (e.g., security-related regulations and laws and new threats) and operations (e.g. changing mission, business practices, upgraded or new technology) affect compliance.

3. Include all organizational safeguards and systems, as well as a review of information systems, in technical and non-technical assessments.

III. Definitions Associated with Security Evaluation

A. Administrative safeguards: Administrative actions, policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the Covered Entity's workforce in relation to the protection of that information.

B. Physical safeguards: Physical measures, policies, and procedures to protect a Covered Entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

C. Technical safeguards: Technology and the policy and procedures for its use that protect electronic health information and control access to it.

D. Covered Entity: A health plan or a healthcare provider who transmits any health information in electronic form in connection with a transaction (see DoD 6025.18-R, paragraph DL1.1.35.) covered by this Regulation, e.g. ACS X12N 837 healthcare claims, ASC X12N 270/271 eligibility inquiries and responses, and the electronic forms of other transactions identified at DoD 6025.18-R, DL1.1.35. In the case of a health plan administered by the Department of Defense, the covered entity is the DoD Component (or subcomponent) that functions as the administrator of the health plan. (See DoD 6025.18-R, paragraph DL1.1.17. for additional information on health plan administrators.) To the extent this Regulation prescribes duties to be performed by covered entities, the term refers only to DoD covered entities. Under subparagraph DoD 6025.18-R, C3.2.2., all covered entities of the Military Health System (MHS) (including both health plans and healthcare providers) are designated as a single covered entity. Not all healthcare providers affiliated with the Armed Forces are covered entities; among those who are not providers associated with Military Entrance Processing Stations (MEPS) and Reserve components practicing outside the authority of military treatment facilities (MTFs) who do not engage in electronic transactions covered by the Regulation.

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.