# TMA Privacy Office Information Paper

# Documentation of Security Actions

**HIPAA Security ♦ September 2012**

## *I. Supporting Regulations and Policies for this Information Paper*

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (45 C.F.R. § 164.316(b)(1)(ii) and (b)(2)) establishes the requirements for documenting security actions.

B. The "DoD Health Information Security Regulation" (DoD 8580.02-R, C1.6.4.5.) implements the above part of the HIPAA Security Rule within the Military Health System (MHS).

C. Administrative Instruction 15, "Office of the Secretary of Defense (OSD) Records Management Program – Administrative Procedures," November 14, 2006, Incorporating Change 1, April 18, 2008.

## *II. Guidance for Documentation of Security Actions*

A. The Security Rule requires covered entities to "maintain the policies and procedures implemented to comply with the [Security Rule] in written (which may be electronic) form" and maintain a "written (which may be electronic) record" of any "action, activity or assessment" that is required by the standards and implementation specifications of the Rule. This standard includes two parts.

B. **Part 1:** The first part requires covered entities to document in written format (paper or electronic) policies and procedures pertaining to the protection of electronic protected health information. When organizations develop and maintain their policies and procedures as part of an "oral tradition" only, they become vulnerable to several threats. Orally developed and transmitted policies tend to drift in response to local circumstances thus helping produce varying practice across the organization. In the absence of written rules, organizations inconsistently and incompletely train personnel and find consistent enforcement difficult or impossible. Maintaining policies and procedures in written format safeguards against these threats.

C. **Part 2:** The second part requires covered entities to document the results of implementing the policies and procedures when required by a standard or implementation specification. The following actions are required to be documented and additional information and requirements can be found in the noted section of the regulations:

1. Decisions regarding addressable implementation specifications, specifically why it would not be reasonable and appropriate to implement the implementation specification in question (45 CFR 164.306(d)(3)(ii)(B)(1)) (DoD 8580.02-R, C1.6.4.3.4.1.);
2. A user's right of access to a workstation, transaction, program, or process (45 CFR 164.308(a)(4)(ii)(C)) (DoD 8580.02-R, C2.5.5.);
3. Security incidents and their outcomes (45 CFR 164.308(a)(6)(ii)) (DoD 8580.02-R, C2.7.2.);
4. Satisfactory assurances that a business associate will appropriately safeguard PHI. This documentation is recorded in a written contract or other arrangement with the business associate and must meet the applicable requirements of business associate agreements. If satisfactory assurances cannot be attained, document the attempt and the reasons that these assurances cannot be obtained (45 CFR 164.308(b)(4) & 45 CFR 164.316(a)(2)(ii)(B)) (DoD 8580.02-R, C2.10.);
5. Repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks) (45 CFR 164.310(a)(2)(iv)) (DoD 8580.02-R, C3.2.6.); and
6. Changes to organizational policies and procedures (45 CFR 164.316(a)) (DoD 8580.02-R, C1.6.)

D. This serves several purposes. Examination of the records for patterns of activity can reveal threats and vulnerabilities, allowing the covered entity to take action to improve the security of protected health information. Because written records demonstrate compliance with policies and procedures, auditors and other surveyors often request to review them during inspections. And finally written records can demonstrate due diligence. Documentation must be "detailed enough to communicate the security measures taken and to facilitate the periodic evaluations" required by the security evaluation standard of the administrative safeguards. See 45 CFR 164.308(a)(8) and DoD 8580.02-R, C2.9.

E. There are three required implementation specifications associated with the documentation standard:

1. Time limit: Retain the documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later

2. Availability: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains

3. Updates: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health

F. These administrative implementation specifications need to be accounted for and incorporated into the documentation lifecycle as determined by the appropriate records disposition schedule and in accordance with Reference (C).

## *III. Definitions Associated with Documentation of Security Actions*

A. 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.

B. Documentation: Written security plans, rules, procedures, and instructions concerning all components of an entity's security program, and written records of any action, activity, or assessment required by HIPAA and DoD 8580.02-R, C1.6.4.5.

C. Security Actions: Any actions, activities or assessments performed within a covered entity in order to comply with the standards and implementation specifications of the HIPAA Security Rule, such as Security incidents and their outcomes, changes to organizational policies, etc.