TMA Privacy and Civil Liberties Office
Information Paper

The Privacy Rule and Documentation

HIPAA Privacy ◆ November 2012

I. Supporting Policies for this Information Paper

A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (45 CFR 164.530(j)) establishes requirements regarding documentation and retention of all HIPAA related activities by a covered entity.

B. The Department of Defense Health Information Privacy Regulation (DoD 6025.18-R, Chapter 14.10) implements the above provision of the HIPAA Privacy Rule within the Military Health System (MHS).

II. Definitions Associated with the Privacy Rule and Documentation

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. Designated Record Set: A group of records that includes:

1. Medical and billing records maintained by or for healthcare provider.
2. The enrollment, payment, claims adjudication, and case or medical management record system maintained by or for a health plan; or
3. Records used, in whole or in part, by or for the covered entity to make decisions about individuals.

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

D. 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 employer.

E. 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 the Privacy Rule and Documentation

A. Documentation of the Privacy Rule. A covered entity shall maintain policies and procedures on the access, use, and disclosure of PHI – in written or electronic form – that are designed to comply with the requirements of the Privacy Rule.

1. If a communication is required to be in writing, a covered entity shall maintain such communication, or an electronic copy, as documentation.

2. If an action, activity, or designation is required to be documented, a covered entity shall maintain a written or electronic record of such action, activity, or designation.

B. Exception. The Privacy Rule does not require a covered entity to document PHI, including oral communication, which is used or disclosed for treatment, payment or healthcare operations.

C. When Documentation is Required. Covered entities are responsible for ensuring the protection of PHI and for maintaining documentation of PHI with regards to individuals' rights. The following are circumstances, related to individual rights, when documentation is required:

1. Authorizations: A covered entity shall document and retain any signed authorization or a revocation of authorization.

2. Notice of Privacy Practice (NoPP). In addition to maintaining copies of the NoPP, a covered entity shall document all written acknowledgments of receipt of the NoPP or document good faith efforts to obtain such written acknowledgments.

3. Restriction of PHI.
    a) A covered entity that agrees to an individual's request for the restriction of the uses and disclosures of their PHI shall document such restriction.
    b) A covered entity that denies an individual's request for the restriction of the uses and disclosures of their PHI shall document such denial.

4. Access of PHI.
    a) A covered entity shall document the designated record sets that are subject to access by individuals.
    b) A covered entity shall document the titles of persons/offices responsible for receiving and processing requests for access to PHI by individuals.
    c) A covered entity shall document requests for access to PHI, including approval and denial of such requests.

5. Amendment of PHI.
    a) A covered entity shall document the titles of persons or offices responsible for receiving and processing requests for amendments.
    b) A covered entity shall document requests for amendments of PHI, including approval and denial of such requests.

6. Accounting of Disclosures.

    a) A covered entity shall document the information required to be included in an accounting of disclosures. Such disclosures include all disclosures of PHI except those noted under paragraph C13.1.

    b) A covered entity shall document the written accounting that is provided to the individual.

    c) A covered entity shall document the titles of the persons or offices responsible for receiving and processing requests for an accounting.

7. Complaints. A covered entity shall document all complaints received and their disposition.

8. Sanctions. A covered entity shall document sanctions that are applied to workforce members who fail to comply with the privacy policies and procedures of the covered entity.

D. Retention Period. A covered entity shall retain the documentation required by the above sections for six years from the date of its creation or the date when it last was in effect, whichever is later.