



# TMA Privacy and Civil Liberties Office Information Paper



## Best Practices for Verification of Identity

HIPAA Privacy ♦ October 2012

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

- A. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (45 CFR 164.514(h)(1)) establishes verification requirements prior to disclosures of protected health information (PHI).
- B. The Department of Defense (DoD) Health Information Privacy Regulation (DoD 6025.18-R) implements the HIPAA Privacy Rule within the Military Health System (MHS).
- C. The DoD Health Privacy Program Regulation (DoD 5400.11-R) sets forth the requirements for protecting and safeguarding an individual's privacy when collecting, maintaining, using, or disseminating personally identifiable information (PII).

### **II. Definitions Associated with Best Practices for Verification of Identity**

- 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. 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. Suggested Best Practices for Verification of Identity

- A. Policies and Procedures. Covered entities should develop and implement reasonable policies and procedures to verify the identity and authority of individuals before granting access to PHI.
1. Covered entities may rely on their professional judgment, as well as industry standards, in designing such policies and procedures.
  2. Identity verification procedures should not be:
    - a) Complicated as to unnecessarily discourage individuals from seeking access to information; or
    - b) Required of an individual seeking access to records that normally would be available under the DoD Freedom of Information Act Program (DoD 5400.7-R).
- B. Requests for Disclosure. Provided that the disclosure of information is permitted under the HIPAA Privacy Rule, an individual may be required to show reasonable proof of his or her identity prior to the disclosure.
1. Examples of requests and identity verification procedures include the following:
    - a) Request made in person. Individuals may present documents which normally provide proof of identity, such as employee and military identification cards, driver's license, passport, or other government issued identification.
    - b) Request by mail. Individuals may need to provide minimum identifying data, such as full name, date and place of birth, or such other personal information only known to the individual.
    - c) Third-party request. Individuals may be required to furnish a signed access authorization granting the third-party access. Examples of third parties who may be requesting records on behalf of the individual include an attorney, an insurance company representative, or a family member or friend of the individual.
    - d) Request by law enforcement. The law enforcement official should present a badge, official identification, or other identification that shows that the official has the authority to accept the PHI on behalf of the law enforcement agency.
    - e) Request on behalf of a minor. Individuals should provide a copy of a birth certificate, a court order, or other competent evidence of the relationship or authority. In addition, the individual should verify his or her own identity with photo identification.
    - f) Request by a healthcare provider. The requesting entity should provide the provider's name, facility name, location, and the telephone number.
  2. An individual may not be refused access to his or her record solely because he or she refuses to provide his or her SSN, unless the SSN is the only method by which retrieval can be made.
- C. Documentation. A covered entity must keep an accounting of disclosures of PHI, except where otherwise noted such as for the purposes of treatment, payment, and healthcare operations.