



VERIFICATION OF IDENTITY PRIOR TO DISCLOSURE OF PHI

HIPAA Privacy ♦ December 2005

Purpose

The purpose of this paper is to provide guidance on the verification of a requestor's identity prior to the release of protected health information (PHI) and to ensure that the Military Health System (MHS) applies appropriate safeguards, as set by the DoD Health Information Privacy Regulation (DoD 6025.18-R) and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. Reasonable efforts must be made to prevent any use or disclosure of PHI which would be in violation of HIPAA. The requirement for identity verification is established by HIPAA at 45 CFR 164.514(h)(1).

Policy

Covered Entities (CE) must verify the identity of any person or entity requesting PHI and the authority of any such person to have access to the requested PHI, if the identity or such authority is not previously known to the MHS.

Guidance

The following guidance should be used to verify the identity of any person or entity requesting PHI:

A. Request Made in Person (Patient Requests):

Patients may request PHI pertaining to themselves be released to themselves or others as they specify. The patient's identity shall be verified.

1. Provide one piece of tangible identification (preferably picture I.D.)
 - Military identification card
 - Individual's drivers license
 - Employment identification card/badge
 - Passport
 - Other government issued identification
2. If an individual is requesting his or her own PHI, the name on the identification must match the name of the individual whose record is being sought.
3. If the patient's name has been legally changed, evidence documenting the name change must be presented.

B. Law Enforcement Requests:

Law enforcement officials and other individuals may request PHI of a beneficiary if they meet the conditions of DoD 6025.18-R, C7.6. If a law enforcement official makes a request, the official must verify his or her identity by producing a badge, official identification, and/or other



TMA Privacy Office Guidance

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



VERIFICATION OF IDENTITY PRIOR TO DISCLOSURE OF PHI

HIPAA Privacy ♦ December 2005

identification that shows that the law enforcement official has the authority to accept the PHI on behalf of the law enforcement agency. The law enforcement official must also produce the official law enforcement request or court order requesting the release of PHI.

C. **Attorney Requests:**

If a patient completes a valid HIPAA compliant authorization (DoD Form 2870, “Authorization for Disclosure of Medical or Dental Information”) for PHI to be disclosed to an attorney, and the attorney comes to the MHS facility in person to pick up the records, the attorney must present valid photo identification and the patient authorization. If a representative of the attorney comes in the attorney’s place, the representative must submit proof that the representative has authority to act on behalf of the attorney (e.g., a designation by the attorney written on corporate letterhead). This provision also applies to patient authorizations to disclose PHI to an insurance company representative among other similar organizations. The type of identification and any documentation of authority used will be documented on the completed HIPAA compliant authorization for each use and disclosure.

D. **Third-party Requests:**

If a patient completes a valid HIPAA compliant authorization for PHI to be disclosed to another individual (e.g., family member or friend), the individual must verify his or her identity with valid photo identification that matches the patient authorization to whom the PHI may be disclosed. The type of identification and any documentation of authority used will be documented on the completed valid HIPAA compliant authorization for use and disclosure.

E. **Requests on Behalf of a Minor:**

If an individual makes a request for PHI on behalf of a minor or for a person where the individual is the legal guardian, the individual must verify that he/she has authority to act by providing a copy of a birth certificate, a court order, or other competent evidence of the relationship or authority (e.g., health care power of attorney), in addition to verifying his/her own identity with photo identification. The type of identification and any documentation of authority used will be documented on the completed HIPAA compliant authorization for use and disclosure.

PrivacyMail@tma.osd.mil ♦ www.tricare.mil/tma/privacy



TMA Privacy Office Guidance

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



VERIFICATION OF IDENTITY PRIOR TO DISCLOSURE OF PHI

HIPAA Privacy ♦ December 2005

F. Request Made by Mail:

Since it is not possible to verify identity through the mail, the following steps shall be taken:

1. If the patient is requesting PHI be sent to him/herself, verify that the name, address, particular information, and signature on the request is the same as those in the patient file. If necessary, contact with the patient may be required. The patient must make the request using a valid HIPAA compliant authorization for use and disclosure.
2. If the patient is requesting PHI be sent to another individual and encloses a valid HIPAA compliant authorization for use and disclosure, verify the identity (in accordance with section F.1. above) and release the information only to the name and address of the individual authorized to receive the PHI in accordance with the patient authorization.
3. If another individual requests (including requests by law enforcement, attorneys, or insurance company representatives) PHI of a patient, the requestor must include documentation of authority (e.g., law enforcement requests must be on letterhead, requests by attorneys must include a valid HIPAA compliant authorization verified in accordance with section F.1. above).
4. If an individual is requesting PHI for a minor or for a person in a situation where the individual is the legal guardian, the requestor must supply a birth certificate, a court order, or other competent evidence of the authority or relationship. The requestor must make the request using a valid HIPAA compliant authorization for use and disclosure, which will be verified in accordance with Section C.1 above.

G. Request by a Healthcare Provider:

Representatives of hospitals, clinics, and health centers may request the release of PHI.

1. Telephone Request Made for Emergency Treatment Purposes.
 - a. Record the provider's name, facility name, location, and the telephone number of the requesting entity.
 - b. Document in the patient record the requesting provider's name, facility name, location, and telephone number and the name of the staff member who received the call on the provider's behalf, the information being sought or requested, and the reason for the request.

PrivacyMail@tma.osd.mil ♦ www.tricare.mil/tma/privacy



TMA Privacy Office Guidance

Records Management ♦ FOIA ♦ DUAs ♦ HIPAA Compliance ♦ Privacy Act/System of Records ♦ PIAs



VERIFICATION OF IDENTITY PRIOR TO DISCLOSURE OF PHI

HIPAA Privacy ♦ December 2005

- c. Provide the PHI that the requesting entity indicates is immediately necessary by telephone at the time of the call. Provide any non-urgent PHI by routine means as would be utilized in a non-emergency circumstance. Note: Do not withhold disclosure of PHI if the entire record is requested/required for medical treatment purposes.
2. Requests by Subpoena/Court Order are to be processed under the specific guidance provided by the local general counsel office or Service policy.
3. Consult with the MTF Medical Record Department/Patient Administration Office and/or legal counsel for information relating to state law or specific requirements to medical record release of information.

H. Recordkeeping:

The Protected Health Information Management Tool (PHIMT) is the preferred recordkeeping source for documentation on how a PHI requestor's identity has been verified. The PHIMT is a centralized repository and can track staff member actions regarding disclosures. The tool simplifies the provision of an accounting of disclosures if a patient makes a request.

In addition to using the PHIMT the MTF shall maintain copies of pertinent documentation in patient records or another central, secure location. Pertinent documentation includes the patient authorization form initialed and dated by the staff member making the verification. The original will be placed in the patient's medical record and a copy provided to the local MTF Privacy Officer.

PrivacyMail@tma.osd.mil ♦ www.tricare.mil/tma/privacy

TMA Privacy Office 5111 Leesburg Pike, Suite 810 Falls Church, VA 22041