Department of Veterans Affairs **VHA DIRECTIVE 2012-036**
Veterans Health Administration
Washington, DC 20420 **December 26, 2012**

IDENTITY AUTHENTICATION FOR HEALTH CARE SERVICES

1. PURPOSE: This Veterans Health Administration (VHA) Directive provides policy and procedures for VHA staff to authenticate the identity of individuals requesting medical care, treatment, or services in person at Department of Veterans Affairs (VA) health care facilities or through telephonic communications with VHA staff. **AUTHORITY: Privacy Act of 1974, Title 5 United States Code (U.S.C.) 552a, Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, Title 45 Code of Federal Regulations (CFR) Part 160 and 164.**

2. BACKGROUND

a. To fulfill its mission of providing health care to Veterans, VHA must establish and maintain a record on each Veteran to establish eligibility and medical history. These records, including administrative data (both static and transient) consisting of demographic information, are "personally identifiable information" (PII) and are protected under Federal laws, such as the Privacy Act of 1974 (Title 5 U.S.C. 552a(e)(10)) and HIPAA Privacy Rule (Title 45 CFR Part 160 and 164), as well as VA policies that establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of PII. VA must protect against any anticipated threats or hazards to the security or integrity of the data, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual for whom information is maintained.

b. **Definitions**

(1) **Administrative Correction.** Administrative correction is the documentation by administrative personnel with the authority to correct information previously captured by, or in, error. For example, a request to change transient administrative data is not an "amendment request," but rather it is an administrative correction as defined in VHA Handbook 1907.01, Health Information Management and Health Records.

(2) **Amendment Request.** Amendment request is a request for the authorization to alter health information by modification, correction, addition, or deletion.

(3) **Authenticate.** Authenticate is defined as to establish that something is genuine; for the purpose of this Directive, to validate the identity of individuals requesting medical care, treatment, or services in person at VA health care facilities or through telephonic communications with VHA staff.

(4) **Challenge Questions.** Challenge questions are defined as questions used to authenticate a Veteran's identity when no acceptable Primary or Secondary Identification Documents are available, or when requests are received by telephone.

(5) **Personal Representative.** A personal representative is a person, who under applicable law, has authority to act on behalf of the individual. This may include power of attorney, legal guardianship of an individual, the executor of the estate of a deceased individual, or someone under Federal, state, local or tribal law with such authority (e.g., parent of a minor).

(6) **Primary Identification Document.** Primary Identification Document is defined as a document used to validate the identity of an individual; the document must be current, valid, and if applicable, contain a recognizable photograph (i.e., State issued drivers license, United States passport).

(7) **Secondary Identification Document.** Secondary Identification Document is defined for the purpose of this Directive, as a document used to validate the identity of an individual, when a primary identification document is not available (i.e., Social Security Card, certified Birth Certificate).

(8) **Static Administrative Data.** Static administrative data is defined as information that normally would not change (i.e., date of birth, place of birth, social security number, or mother's maiden name).

(9) **Transient Administrative Data.** Transient administrative data is defined as information that is not fixed and could be changed at will (i.e., address, phone number).

c. To ensure that VHA is taking every precaution to protect the identity of Veterans and other beneficiaries accessing VA health care services and the integrity of electronic data, this Directive establishes requirements for authenticating the identity of Veterans or others who request changes, on behalf of Veterans, to both static and transient administrative data.

3. POLICY: It is VHA policy that VHA staff authenticates the identity of any individual requesting services or changes to any PII.

4. ACTION

a. **Facility Director.** Each facility Director is responsible for ensuring that:

(1) Facility staff authenticates the identity of Veterans who enroll in person, or who are accessing VA health care services for the first time, by requesting a Primary Identification Document (see Att. A).

(2) Veterans or other beneficiaries are not turned away solely because they cannot provide the required Primary Identification Document. VA staff must attempt to authenticate an individual's identity by asking the Veteran or other beneficiary to:

(a) Provide two Secondary Identification Documents, or

(b) Respond to a series of verifiable challenge questions (see Att. A).

(3) A Veterans Identification Card (VIC) is not created until the Veteran's identity is authenticated and eligibility has been verified.

(4) Facility staff update the Veteran's static administrative data only upon receipt of a written request signed by the Veteran or during an in-person visit where the Veteran's identity has been verified. Requests to change static administrative data are considered to be "amendment requests" and may be made only by the Veteran or by a "personal representative" of the Veteran, as defined in VHA Handbook 1605.1, Privacy and Release of Information. Appropriate supporting documentation for the update must accompany this request.

(5) Facility staff may update a Veteran's transient administrative data when the request is received from the Veteran, or from an individual known to be involved in the Veteran's care or payment for care. If a request is received by telephone, facility staff must determine that the individual making the request is the Veteran or a person authorized to act on the Veteran's behalf by soliciting correct answers to a series of challenge questions (see Att. A).

NOTE: *For procedures on documentation necessary to change any administrative data, refer to VHA Handbook 1605.1.*

(6) Veterans who have been enrolled in the system and are presenting for care show a Primary Identification Document (see Att. A). If the Veteran does not have a valid Primary Identification Document, the Veteran must be asked to:

(a) Provide two Secondary Identification Documents, or

(b) Answer a series of verifiable challenge questions (see Att. A).

(7) Any facility staff suspecting, for any reason, that a person may be fraudulently receiving VA health care benefits, must immediately notify their supervisor, Chief of Health Information Management (HIM), and the Business Office Manager, or equivalent.

(8) Disclosures of sensitive information are made in accordance with VHA Handbook 1605.1. When disclosures are to be made verbally, the Veteran must be offered a safe and secure area designed to promote privacy (i.e., private office).

b. **Supervisor, Chief of Health-care Identity Management (HIM), and/or Business Office Manager.** The supervisor, Chief of HIM, and/or Business Office Manager, or equivalent, is responsible for:

(1) Notifying the VHA Health-care Identity Management Team of suspected fraudulent incidents, preferably by using their local Master Patient Index (MPI) point of contact.

(2) Initiating appropriate notification of management staff, police, the local Information Security Officer, the local Privacy Officer, appropriate Regional Counsel, and the Office of Inspector General (OIG) to conduct necessary investigation(s) and background verification of any reported suspicion of identity fraud.

c. **Consolidated Patient Accounts Center (CPAC) Director.** Each CPAC Director is responsible for ensuring that CPAC Staff:

(1) Determine the individual making the request is the Veteran or Veteran's representative authorized to act on the Veteran's behalf, by using the appropriate method as outlined in Att. A.

(2) Follow the Accounting of Disclosure procedures in accordance with VHA Handbook 1605.1 if releasing PII.

(3) Assist with resolution of identified patient information discrepancies by referring Veterans and/or documentation to the appropriate department for resolution as outlined in VHA Handbook 1907.01

(4) Report any suspected fraudulent representations immediately to their supervisor, CPAC leadership, and/or CPAC Privacy Officers as appropriate.

d. **Health Resource Center (HRC) Director.** Each HRC Director is responsible for ensuring that staff follows policy set forth in this Directive.

5. REFERENCES

a. Title 38 U.S.C. Chapter 17.

b. Title 38 CFR Part 17.

c. Privacy Act of 1974, 5 U.S.C. 552a.

d. HIPAA Privacy Rule, 45 CFR part 160 and 164.

e. VHA Handbook 1605.1, Privacy and Release of Information.

f. VHA Handbook 1907.01, Health Information Management and Health Records.

6. FOLLOW-UP RESPONSIBILITY: The Chief Business Office (10NB) is responsible for the contents of this Directive. Questions may be addressed at 202-461-1589.

7. RESCISSIONS: VHA Directive 2007-037, Identity Authentication for Health Care Services, is rescinded. This VHA Directive expires on December 31, 2017.

Robert A. Petzel, M.D.
Under Secretary for Health

Attachment

DISTRIBUTION: E-mailed to the VHA Publications Distribution List 12/28/2012

ATTACHMENT A

PROOF OF IDENTIFICATION DOCUMENTS

1. Primary Identification Documents. The following are sources of identification (ID):

NOTE: *The identification must be current, valid, and contain, as applicable, a recognizable photograph.*

a. State issued Drivers License,

b. State issued ID,

c. United States (U.S.) Passport (Non-citizens may provide a foreign passport),

d. Department of Veterans Affairs (VA) Identification Card (VIC),

e. Military ID Card (DD Form 2 or DD Form 1173),

f. Temporary Resident ID Card (I-688),

g. Resident Alien Card (old version of I-551),

h. Permanent Resident Card (current version of I-551), or

i. Other Federal or State issued ID.

2. Secondary Identification Documents. Two of the following documents are required for initial verification, if a primary document is not available.

a. Certified Birth Certificate,

b. Social Security Card (original, not a metal or plastic facsimile),

c. Department of Defense Form DD214, Certificate of Release or Discharge from Active Duty; or equivalent certificate issued by a uniformed service, Department of Defense, or War Department containing the full name of the service member, branch of service, active duty or reserve status, beginning and ending dates of service, and character of discharge,

d. Marriage License (certified copy of license filed with the clerk of court),

e. Voter Registration Card,

f. Student ID Card,

g. Native American Tribal Document,

h. Certificate of U.S. Citizenship (Immigration and Naturalization Service (INS) Forms N-560, N-561, or N-645);

i. Certificate of Naturalization (INS Forms N-550, N-570, or N578), and

j. Any of the following certificates issued by US Consular Offices documenting the birth of a child on foreign soil to a US citizen:

(1) Certification of Birth Abroad (FS Form 545),

(2) Certification of Birth Abroad (DS Form 1350),

(3) Certification of Report of Birth,

(4) Consular Report of Birth Abroad (FS Form 240), or

(5) Report of Birth: Child Born Abroad of American Parent or Parents (DS Form 240).

NOTE: *If a name change has occurred as a result of marriage, divorce, court order, or as part of the naturalization process, official documentation is required.*

3. Challenge Questions. These questions are to be used to authenticate a Veteran's identity when no acceptable Primary or Secondary Identification Documents are available, or when requests are received by telephone.

a. Staff must ask questions that are verifiable through existing Veterans Health Information and Technology Architecture **(**VistA) entries, Hospital Inquiry (HINQ), Veterans Information System (VIS), or other reliable sources. Ask only as many questions as necessary to positively authenticate the Veteran's identity (usually three or four), however, full legal name, including middle name (if one exists), is a required question and must be asked in addition to at least two of the following questions.

b. Ask the Veteran, or person acting on behalf of the Veteran, to provide the Veteran's:

(1) Full legal name, including middle name,

(2) Social Security Number (SSN), ***NOTE:*** *Although VA has indicated it will not call a Veteran and ask for a SSN, it is allowable to ask for a SSN when the Veteran (or someone on the Veteran's behalf) initiates the call or is presenting in person.*

(3) Military Service Number,

(4) VA Claim Number,

(5) Branch of service and service dates,

(6) Birth date, including year,

(7) Place of birth, the city and state,

(8) Home address,

(9) Spouse's name,

(10) Mother's maiden name,

(11) Next of kin.

4. Sample Scenarios. The following is a table of the different scenarios that may take place and the action that is to be taken by the person on staff asking the challenge questions.

	Scenario	**Action**
1	Veteran refuses to answer question.	Ask another question.
2	Veteran does not remember (e.g., Military Service Number).	Ask another question.
3	Veteran refuses to answer all questions, cannot remember the answers to the three or four questions, or answers incorrectly.	Care will not be provided, unless emergent care is required, until identification can be verified.