Department of Veterans Affairs **VHA DIRECTIVE 2007-037**
Veterans Health Administration
Washington, DC 20420 **November 6, 2007**

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 at Department of Veterans Affairs (VA) health care facilities.

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 United States Code (U.S.C.) 552a(e)(10)) and Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (Title 45 Code of Federal Regulations (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. The Office of the Inspector General (OIG) has reported that VA has experienced a number of cases of identity theft in recent years. Currently, VA lacks the requirements for staff to authenticate veteran or beneficiary identity when they are accessing or otherwise interacting with the VA health care system. Additionally, when an individual contacts VA by phone requesting changes in administrative information, no national policy or procedure is in effect to guide staff in authenticating the identity or authority of this individual to make such changes.

d. **Definitions**

(1) For the purposes of this Directive, "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).

(2) For purposes of this Directive, "transient administrative data" is defined as information that is not fixed and could be changed at will (i.e., address, phone number).

(3) A request to change transient administrative data is not an "amendment request," but rather it is an administrative correction as defined in VHA Handbook 1907.1.

e. 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 authenticate the identity of individuals 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.

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

(5) Veterans who have been enrolled in the system and are presenting for unscheduled 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).

(6) 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).

(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 HIM, and/or Business Office Manager.** The supervisor, Chief of HIM, and/or Business Office Manager, or equivalent, is responsible for:

(1) Notifying the National Identity Management Data Quality 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 OIG to conduct necessary investigation(s) and background verification of any reported suspicion of identity fraud.

5. REFERENCES

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

b. Title 38 CFR Part 17.

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

d. Office of Inspector General, Semiannual Report to Congress, April 1, 2003 – September 30, 2003.

6. FOLLOW-UP RESPONSIBILITY: The Chief Business Office (16) is responsible for the contents of this Directive. Questions may be referred to (202) 254-0486.

7. RESCISSIONS: None. This VHA Directive expires November 30, 2012.

Michael J. Kussman, MD, MS, MACP
Under Secretary for Health

Attachment

DISTRIBUTION: CO: E-mailed 11/7/07
FLD: VISN, MA, DO, OC, OCRO, and 200 – E-mailed 11/7/07

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,

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

e. Military ID Card,

f. Temporary Resident ID Card,

g. Resident Alien Card,

h. Permanent Resident Card, or

i. Other Federal or State recognized 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;

c. Department of Defense Form DD214, Certificate of Release or Discharge from Active Duty;

d. Marriage License;

e. Naturalization Certificate;

f. Voter Registration Card;

g. Student ID Card;

h. Native American Tribal Document;

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

j. Certificate of Naturalization (INS Forms N-550 or N-570); and

k. Certification of Birth Abroad Issued by the Department of State (Foreign Service (FS) Form 545, Certification of Birth Abroad, or Department of State (DS) Form 1350, Certification of Report of Birth.

NOTE: *If a name change has occurred, 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 two or three 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.