Department of Veterans Affairs
Veterans Health Administration
Washington, DC 20420

VHA DIRECTIVE 1907.09
Transmittal Sheet
June 6, 2019

IDENTITY AUTHENTICATION FOR HEALTH CARE SERVICES

1. REASON FOR ISSUE: This Veterans Health Administration (VHA) directive provides policy and required 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.

2. SUMMARY OF MAJOR CHANGES: This VHA policy revises and updates the requirements VHA Directive 2012-036, dated December 26, 2012.

3. RELATED ISSUES: VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016; and VHA Handbook 1907.01, Health Information Management and Health Records, dated March 19, 2015.

4. RESPONSIBLE OFFICE: The Member Services Business Policy Office (10NF) is responsible for the content of this directive. Questions related to the Identity Authentication for Health Care Services may be referred to the Member Services Business Policy Office at VHAMSBusinessPolicyOffice@va.gov.

5. RESCISSION: VHA Directive 2012-036, Identity Authentication for Health Care Services, dated December 26, 2012, is rescinded.

6. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last working day of June 2024. This VHA directive will continue to serve as national VHA policy until it is recertified or rescinded.

BY DIRECTION OF THE OFFICE OF
THE UNDER SECRETARY FOR HEALTH:

Renee Oshinski
Acting Deputy Under Secretary for
Health for Operations and Management

NOTE: *All references herein to VA and VHA documents incorporate by reference subsequent VA and VHA documents on the same or similar subject matter.*

DISTRIBUTION: Emailed to the VHA Publications Distribution List on June 11, 2019.

CONTENTS

IDENTITY AUTHENTICATION FOR HEALTH CARE SERVICES

IDENTITY AUTHENTICATION FOR HEALTH CARE SERVICES

1. PURPOSE

This Veterans Health Administration (VHA) directive provides the policy and responsibilities 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: Title 5 United States Code (U.S.C.) 552a, Title 38 Code of Federal Regulations (C.F.R.) 1.576 and 1.579, and 45 CFR Parts 160 and 164.

2. BACKGROUND

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 contain "personally identifiable information" (PII), and the confidentiality of this information is protected under Federal laws, such as the Privacy Act of 1974, 5 U.S.C. 552a (e) (10), and the HIPAA Privacy Rule, 45 CFR Part 160 and 164. In addition, VA and VHA policies establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of PII. VA must protect PII against any anticipated threats or hazards to the security or integrity of the data, as any breach could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual whose information is compromised.

3. DEFINITIONS

a. **Administrative Correction.** An 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, dated March 19, 2015, or subsequent policy.

b. **Amendment Request.** An amendment request is a request for authorization to alter health information by modification, correction, addition, or deletion.

c. **Authenticate.** Authenticate means to establish that something is genuine. For this directive, authenticate means to validate the identity of an individual requesting medical care, treatment, or services in person at a VA health care facility or through telephonic communications with VHA staff.

d. **Challenge Questions.** Challenge questions are 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.

e. **Personal Representative.** A personal representative is a person, who under applicable law has authority to act on behalf of the individual, to include privacy-related matters. The authority may include power of attorney, legal guardianship of the

individual, appointment as executor of the estate of a deceased individual, or a Federal, state, local, or tribal law that establishes such authority (e.g., parent of a minor).

f. **Personally Identifiable Information.** Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be PII. ***NOTE:*** *The term "personally identifiable information" is synonymous with "sensitive personal information."*

g. **Primary Identification Document.** A primary identification document is 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 Driver's License, United States Passport, see Appendix A).

h. **Secondary Identification Document.** A secondary identification document is 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, see Appendix A).

i. **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).

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

4. POLICY

To ensure Veterans receive appropriate treatment and protect privacy, it is VHA policy that VHA staff must authenticate the identity of any individual requesting services. ***NOTE:*** *For information regarding changes to PII, see VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016.*

5. RESPONSIBILITIES

a. **Under Secretary for Health.** The Under Secretary for Health is responsible for ensuring overall VHA compliance with this directive.

b. **Deputy Under Secretary for Health for Operations and Management.** The Deputy Under Secretary for Health for Operations and Management is responsible for communicating the contents of this directive to all Veterans Integrated Services Networks (VISN).

c. **Veterans Integrated Network Director.** The VISN Network Director is responsible for:

(1) Ensuring that each facility within their VISN has sufficient resources to fulfill the terms of this directive; and

(2) Providing oversight of facility operations to ensure compliance with all applicable statutes, regulations, VA and VHA policies.

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

e. **Health Eligibility Center Director.** The Health Eligibility Center (HEC) Director is responsible for ensuring that HEC staff follows policy set forth in this directive.

f. **VA Medical Facility Director.** Each VA medical facility Director or designee is responsible for ensuring that facility staff adheres to authentication processes.

g. **Supervisor, Chief of Health-care Identity Management and/or Business Office Manager.** The Supervisor, and/or Business Office Manager, or equivalent, is responsible for:

(1) Notifying the VHA Identity Management Team of suspected fraudulent incidents that have been reported by facility staff, preferably by using their local Master Veteran Index (MVI) point of contact.

(2) Notifying management staff, police, the local Information Security Officer, the local Privacy Officer, Chief Counsel in the District, and the Office of Inspector General (OIG) of any reported suspicion of identity fraud to conduct necessary investigation(s).

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

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

(2) Follow the Accounting of Disclosure procedures in accordance with VHA Directive 1605.01, 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, Health Information Management and Health Records, dated March 19, 2015.

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

i. **Facility Staff.** Facility staff is responsible for:

(1) Authenticating the identity of Veterans or dependents who are registering for VA health care in person, who are accessing VA health care services for the first time, or who are enrolled in the VA health care system already and are presenting for care, by requesting one Primary Identification Document (see Appendix A).

(2) Attempting to authenticate the Veteran or other beneficiary identity if they cannot provide the required Primary Identification Document 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 Appendix A).

(3) Creating a Veterans Health Identification Card (VHIC), once the Veteran's identity is authenticated and eligibility has been verified.

(4) Updating 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 amendment requests as defined in this directive and may be made only by the Veteran or by a personal representative of the Veteran. Appropriate supporting documentation for the update must accompany this request.

(5) Updating 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 Appendix A).

NOTE: *For procedures on documentation necessary to change any administrative data, refer to VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016.*

(6) When, for any reason, an individual is suspected of fraudulently receiving or attempting to receive VA health care benefits, immediately notifying their supervisor, the Chief of Health Information Management (HIM), and the Business Office Manager, or equivalent.

(7) Ensuring disclosures of PII are only made in accordance with VHA Directive 1605.01, or subsequent policy. 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).

6. TRAINING REQUIREMENTS

The following training is recommended for all Identity Authentication for Health Services:

a. **TMS Course Number 7861.** Prevention of Catastrophic Edits to Person Identity. This course should be assigned to all new employees with the responsibility of entering and editing patient data in the ES or VistA system. Those employees are required to take this training and successfully pass the associated competency exam, with an 80 percent or higher score. This will ensure that employees possess the knowledge and skills to prevent these catastrophic edits.

b. **TMS Course Number 29287.** Prevention of Catastrophic Edits to Person Identity-Refresher. This new refresher course will be required of any employee responsible for causing a catastrophic edit or merge. Again, the employee should pass the associated competency exam, with an 80 percent or higher score.

7. RECORDS MANAGEMENT

All records regardless of format (paper, electronic, electronic systems) created by this directive shall be managed per the National Archives and Records Administration (NARA) approved records schedules found in VA Records Control Schedule 10-1, Chapter 6, 6000 series. If you have any questions regarding any aspect of records management you should contact your facility Records Manager or your Records Liaison. Any change to the record disposition schedules of these records shall be coordinated with the Program Office and VHA Records Officer.

8. REFERENCES

a. 5 U.S.C. 552a.

b. 38 CFR 1.575.

c. 38 CFR 1.576.

d. 45 CFR Parts 160 and 164.

e. VHA Directive 1605.01, Privacy and Release of Information.

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

PROOF OF IDENTIFICATION DOCUMENTS

1. PRIMARY IDENTIFICATION DOCUMENTS. The following are sources of primary identification (ID):

a. State issued Driver's License,

b. State issued ID,

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

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

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 issued ID.

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

2. SECONDARY IDENTIFICATION DOCUMENTS. Two of the following documents are required 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 of the name change 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; 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. The staff member should only ask for the Veteran's SSN if there are no other available questions.*

(3) Military Service Number,

(4) Branch of service and service dates,

(5) Birth date, including year,

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

(7) Home or mailing address,

(8) Spouse's name,

(9) Mother's maiden name, and

(10) 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.