

**ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION
IN INFORMATION TECHNOLOGY SYSTEMS**

- 1. REASON FOR ISSUE:** This Veterans Health Administration (VHA) Directive establishes policy for approving and providing authorized users access to VHA personally identifiable information (PII) in Information Technology (IT) systems of the Department of Veterans Affairs (VA).
- 2. SUMMARY OF CHANGES:** This is a new Directive.
- 3. RELATED ISSUES:** VHA Handbook 1080.01, Data Use Agreements.
- 4. RESPONSIBLE OFFICE:** The Director, National Data Systems (10P2C) is responsible for the content of this Directive. Questions may be referred to the Deputy Director, National Data Systems at 202-465-1581.
- 5. RESCISSIONS:** None.
- 6. RECERTIFICATION:** This VHA Directive is scheduled for recertification on or before the last working day of November 2018.

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

DISTRIBUTION: E-mailed to the VHA Publications Distribution List on 11/22/13

ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION IN INFORMATION TECHNOLOGY SYSTEMS

1. PURPOSE: This Veterans Health Administration (VHA) Directive establishes policy for approving and providing authorized users access to VHA personally identifiable information (PII) in Information Technology (IT) systems of the Department of Veterans Affairs (VA). IT systems in operation in VHA are owned and generally managed by the VA Office of Information and Technology (OIT), while the data maintained in the IT systems is owned by VHA. This Directive establishes the policy by which VHA, as the data owner, must approve and provide, where appropriate, authorized users access to VHA III in VA IT systems. **AUTHORITY:** Title 5 United States Code (U.S.C.) 552a(e)(10); 45 CFR parts 160 and 164; and 38 CFR 14.626-14.637.

2. BACKGROUND:

a. Privacy Act of 1974, at 5 U.S.C. 552a(e)(10), states that, “agencies shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.” With the enactment of the Privacy Act, Congress required agencies to employ reasonable technological safeguards to protect PII that is stored electronically.

b. The Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, and its implementing regulations, at 45 CFR parts 160 and 164, include requirements to ensure the security and privacy of personally identifiable health information called protected health information (PHI) by those entities subject to, in relevant part, the Privacy, Security, Enforcement and Data Breach Notification Rules. Security standards under the HIPAA Security Rule, as amended by the Health Information Technology for Economic Health Act enacted under Title XIII of the American Recovery and Reinvestment Act of 2009, and HITECH’s Omnibus Rule of January 23, 2013 apply to all PHI pertaining to an individual that is held or transferred electronically. HIPAA’s Privacy Rule published in 2000 and amended most recently by the Omnibus Rule, establishes standards for the use and disclosure of PHI.

c. Under the provisions of 38 CFR 14.626-14.637, qualified organizations outside VA may be granted recognition by VA to assist Veterans in the preparation, presentation, and prosecution of claims for Veterans’ benefits. This regulatory section outlines the requirements for recognition and defines the process by which representatives of a recognized organization may become accredited by VA. Accredited representatives of Veterans Service Organizations (VSO) possessing a Power of Attorney (POA) or formal written authorization, on behalf of a particular Veteran, are authorized to obtain access to all information in that particular Veteran’s record in accordance with VA/VHA privacy and security policies.

3. POLICY: It is VHA policy that only Authorized Users, appropriately approved and satisfying all VA and VHA policy requirements, are granted access to VHA PII in VA IT systems (see paragraph 6b).

NOTE: This Directive does not negate any existing authority permitting a VA or VHA Program Office to use or obtain VHA PII. This Directive, and corresponding VHA Handbook 1080.01, only outline the policy and process requirements for granting access to VHA PII in VA IT systems. This policy does not encompass VHA PII contained in Medical Devices or on paper.

4. RESPONSIBILITIES:

a. **Assistant Deputy Under Secretary for Health for Informatics and Analytics.** The Assistant Deputy Under Secretary for Health for Informatics and Analytics (OIA) is responsible for:

(1) Ensuring VHA-wide requirements for access to VHA PII are established in accordance with Federal laws, regulations, and VA and VHA policies.

(2) Providing sufficient resources to maintain an oversight function to manage access to VHA information.

b. **Director, National Data Systems.** The Director, National Data Systems (NDS) is responsible for:

(1) Ensuring the Deputy Director, NDS administers the Health Information Access (HIA) Program in furtherance of VHA's mission.

(2) Ensuring policies and procedures establishing VHA-wide requirements to authorize access to VHA PII in VA IT systems are established in accordance with Federal laws, regulations, and VA and VHA policies.

c. **Director of Health Care Security Requirements.** The Director of Health Care Security Requirements is responsible for verifying that agreements for use of VHA PII with entities outside VHA, or internally as required by VHA policy, are in compliance with Federal security law, as well as VA and VHA security policy.

d. **Deputy Director, NDS.** The Deputy Director, NDS is responsible for:

(1) Establishing and maintaining VHA-wide requirements for access to VHA PII in accordance with Federal law and regulation, as well as VA and VHA policies.

(2) Establishing and distributing policies and procedures to authorize access to VHA PII in VA IT systems. Policies and procedures require VHA to determine whether an individual requesting access is an Authorized User before granting access to VHA PII by applying the following criteria:

(a) Verifying that the requestor has legal privacy authority to access VHA PII under Federal law and regulation, as well as VA and VHA policies.

(b) Verifying that the requestor has completed VHA privacy training, if applicable, in accordance with VHA Directive 1605.

(c) Verifying that the requestor has completed applicable VA information security training, in accordance with VA Directive 6500.

(d) Verifying that the requestor has signed the National Rules of Behavior or other approved Rules of Behavior document.

(e) Verifying that the requestor, if not a VA employee, is covered under a valid Business Associate Agreement, contract, Cooperative Research and Development Agreement, or other approved written agreement, if applicable, in accordance with VHA Handbook 1605.1, Privacy and Release of Information.

(f) Verifying that data requests from entities outside VHA meet VHA privacy criteria and comply with applicable legal privacy authority for the disclosure.

(g) Verifying that data requests from VA researchers meet VHA privacy criteria, when a privacy review is required by VA or VHA policy.

(3) Establishing policies and process for the auditing of authorized user access on an ongoing basis to ensure compliance with VA and VHA policy and performing audits, as needed.

(4) Establishing formal processes for VHA Data Owners to ensure Special Users have access to VHA PII in VA IT systems.

(5) Approving, establishing and/or managing access to VHA PII through CAPRI, the Veterans Health Information Systems and Technology Architecture Web (VistAWeb) or other HIA managed IT systems for Special Users.

e. **Veterans Integrated Service Network and VA Medical Facility Directors.** Veterans Integrated Service Network (VISN) and VA medical facility Directors are responsible for:

(1) Establishing a process for ensuring access to any PII in their respective facilities is granted in accordance with VA and VHA policy and this Directive.

(2) Ensuring all medical facility staff only access VHA PII in the performance of their official duties.

(3) Auditing Authorized User access on an ongoing basis to ensure compliance with VA and VHA policy.

f. **Authorized Users.** Authorized users are responsible for:

(1) Ensuring that access to VHA PII is requested and performed in accordance with VA and VHA policy and only for purposes for which access was granted.

(2) Reporting any security or privacy incidents resulting from access to VHA PII in VA IT systems in accordance with VA policy and the National Rules of Behavior.

g. **Special Users.** Special users are responsible for:

(1) Ensuring that access to VHA PII is requested and performed in accordance with VA and VHA policy and only for purposes for which access was granted.

(2) Notifying VHA Data Owner if access to VHA PII is no longer needed or the Special User's official job duties change.

(3) Notifying VHA HIA if access to VHA PII through CAPRI or VistAWeb is no longer needed or the Special User's official job duties change.

(4) Reporting any security or privacy incidents resulting from access to VHA PII in VA IT systems in accordance with VA policy and the National Rules of Behavior.

5. REFERENCES: These references contain all the requirements for authorized users:

a. 38 U.S.C. 7332.

b. 38 CFR. 14.626-14.637.

c. 38 U.S.C. 5721 et seq.

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

e. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191 and its implementing regulations at 45 CFR parts 160 and 164.

f. VA Directive and Handbook 0710, Personnel Suitability and Security Program

g. VA Directive 6500, Manage Information Security Risk: VA Information Security Program.

h. VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program.

i. VA Directive 6502, VA Enterprise Privacy Program.

- j. VHA Directive 1605, VHA Privacy Program.
- k. VHA Handbook 1605.1, Privacy and Release of Information.
- l. VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information.
- m. Memorandum from Office of General Counsel (02) to Under Secretary for Health (10), “Request for Advisory Opinion – Department Information Ownership”, dated December 31, 2007.

6. DEFINITIONS:

a. **Access.** Access is the viewing, inspecting or obtaining a copy, of VHA PII or PHI electronically, on paper or other medium.

b. **Authorized User.** An authorized user is:

- (1) An individual permitted by:
 - (a) Federal law and regulation to have access to or obtain a copy of VHA PII or PHI;
 - (b) VA to have access to one or more VA IT systems; and
 - (c) VHA, in accordance with all applicable VHA policy, and with a need to know to have access to VHA PII or PHI.
- (2) Authorized users may request access to VHA PII and PHI at the local level from a VA medical facility or VISN, or at a national level from a VHA Data Owner (e.g., Decision Support System).
- (3) Authorized users include, but are not limited to, VA employees, VA contractors (including External Peer Review Program), VA Business Associates (including The Joint Commission), volunteers, trainees, students, accredited VSO representatives with a POA, and Department of Defense (DoD) health care staff.

c. **Data Owner.** For the purposes of this Directive, a Data Owner is an agency official with statutory or operational authority over specified information, and responsibility for establishing the criteria for its creation, collection, maintenance, processing, dissemination, or disposal. A Data Owner, or designee, is also an agency official who has been identified as having the responsibility and the accountability for the use or disclosure of the VHA data contained in a VA IT system. These responsibilities may extend to interconnected systems or groups of interconnected systems. As determined by the Office of General Counsel (OGC), the official owner of data within VHA is the Under Secretary for Health. It is VHA practice to delegate responsibility and accountability for business functions and the data related to those functions to

designated VHA Program Offices. Identification of a data owner should generally begin with the program office which sponsored the creation of the data.

d. **Personally Identifiable Health Information.** Personally Identifiable Health Information (PHI) is a subset of Health Information, including demographic information collected from an individual, that: (1) is created or received by a health care provider, health plan, or health care clearinghouse (e.g., a HIPAA-covered entity, such as VHA); (2) relates to the past, present, or future physical or mental condition of an individual, or provision of or payment for health care to an individual; and, (3) identifies the individual or where a reasonable basis exists to believe the information can be used to identify the individual. *NOTE: VHA uses the term PHI to define information covered by the Privacy Act and the Title 38 confidentiality statutes in addition to HIPAA.*

e. **Personally Identifiable Information.** Personally Identifiable Information (PII) is any information pertaining to an individual that is retrieved by the individual's name or other unique identifier, as well as PHI regardless of how it is retrieved. PII is a subset of personally identifiable information and is protected by the Privacy Act.

f. **Protected Health Information.** The HIPAA Privacy Rule defines Protected Health Information (PHI) as PII transmitted or maintained in any form or medium by a covered entity, such as VHA. *NOTE: VHA uses the term protected health information to define information that is covered by HIPAA but, unlike PII, may or may not be covered by the Privacy Act or Title 38 confidentiality statutes. In addition, PHI excludes employment records held by VHA in its role as an employer.*

g. **Special User.** An authorized user whose needs require specialized access to VHA PII or PHI, such as broad access to electronic health records beyond the local level (e.g., national level access to the Compensation and Pension Records Interchange (CAPRI)) or at a very discreet, highly-controlled individual patient level. A special user may be, but is not necessarily, a VA employee. Special users may include, but are not limited to, the VHA Office of Quality and Safety, VA OGC, VA Office of the Inspector General (OIG), DoD, and VSOs. Special users are managed at a national level by the VHA National Data Systems (NDS), Health Information Access (HIA) Program. *NOTE: Access provided at the local level is not considered special user access.*

h. **VA Information Technology System.** For the purposes of this Directive, VA IT Systems are any electronic systems containing PHI or PII belonging to VHA that are maintained by either VA or VHA.