Department of Veterans Affairs
Veterans Health Administration
Washington, DC 20420

VHA DIRECTIVE 1080
Transmittal Sheet
January 6, 2017

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 access to VHA personally identifiable information (PII), including Personal Health Information (PHI), in Information Technology (IT) systems of the Department of Veterans Affairs (VA).

2. SUMMARY OF MAJOR CHANGES: Major updates include new assignments of responsibilities and access roles for clinical staff and clinical support staff.

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 RESCISSIONS: VHA Directive 1080, dated November 20, 2013, is rescinded.

6. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last working day of January 2022. This VHA directive will continue to serve as national VHA policy until it is recertified or rescinded.

David J. Shulkin, M.D.
Under Secretary for Health

DISTRIBUTION: Emailed to the VHA Publications Distribution List on January 10, 2017.

CONTENTS

ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION IN INFORMATION TECHNOLOGY SYSTEMS

ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION IN INFORMATION TECHNOLOGY SYSTEMS

1. PURPOSE

This Veterans Health Administration (VHA) directive establishes policy for approving and providing access to VHA personally identifiable information (PII), including personal health information (PHI), in Department of Veterans Affairs (VA) Information Technology (IT) systems in operation within VHA business lines. These IT systems are owned and generally managed by the VA Office of Information and Technology (OI&T), while the data maintained in the IT systems is owned by VHA. This directive establishes the policy by which VHA, as the data owner, will approve and provide, where appropriate, individuals requesting access to VHA PII in VA IT systems. **AUTHORITY:** Title 5 United States Code (U.S.C.) 552a(e)(10); Title 45 Code of Federal Regulations (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 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. Public Law 113-66, the National Defense Authorization Act of 2014, mandates an integrated data and document display between VA and Department of Defense (DoD). The paradigm shift outlined in the Essential Strategies of the VHA Blueprint for Excellence and the goals of FY2014-2020 VA Strategic Plan will require national/interagency level access to complete VA patient health records.

d. 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.

e. Joint Legacy Viewer (JLV) electronic health record (EHR) was implemented by the Department of Veterans Affairs (VA) to reach its interoperability requirements. JLV has the interoperable functions of an EHR, helping providers see an entire patient's medical history, thus enabling better informed care decisions. JLV has been implemented in 1,700 of VA's health care facilities nationwide, and is being used by nearly 100,000 individuals, helping to connect patient information between multiple VA providers and civilian providers where applicable.

f. Enterprise Health Management Platform (eHMP) will provide end user clinical encounter and care coordination transaction capabilities, data visualization, and decision support integration between provider, patient, and system facing components and devices. Different capability configurations will be available based on user roles. The eHMP will build on the JLV, and maintain the joint VA/DoD JLV functionality.

3. DEFINITIONS

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

b. **Administrative User.** For the purposes of this directive, an administrative user :

(1) Is 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 for multiple purposes including but not limited to: health benefits administration, quality assessment and improvement, operational reporting, compliance and oversight, security and preparedness, application of healthcare ethics standards, cost accounting, auditing, and general administrative duties not generally associated with clinical care.

(2) Includes, but is not limited to, Office of Community Care, VA Police Services, Office of Quality and Performance, National Center for Ethics in Healthcare, VA Health Economic Resource Center.

c. **Advanced Transactional Auditing and Access Control.** IT Systems capabilities that automatically create a continuous record of user system actions and provides the ability to restrict individual user access. The Joint Legacy Viewer and Enterprise Health Management Platform meet these criteria.

d. **Clinical Staff and Clinical Support Staff.** For the purposes of this directive, clinical staff and clinical support staff 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 related to treatment, payment, or health care operations, to have access to VHA PII or PHI.

(2) An individual permitted national level access to VHA PII in VA IT systems, given that the system capabilities include:

(a) Transactional audit log capability; and

(b) Access control capability.

(3) An individual who is VA personnel, including VA employees, without compensation (WOC) clinicians, and medical students.

e. **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.

f. **Electronic Protected Health Information.** Under the HIPAA Privacy Rule electronic protected health information (ePHI) is any individually identifiable health information protected health information that is transmitted by electronic media or maintained in electronic media. The HIPAA Security Rule expands this definition to include all individually identifiable health information for a covered entity such as what VA produces, saves, transfers, or receives in electronic form. ***NOTE:*** *VHA uses the term "protected health information" to define information covered by the Privacy Act and the Title 38 confidentiality statutes in addition to HIPAA. In addition, PHI excludes employment records held by VHA in its role as an employer.*

g. **National Level Access.** Access to health records of all VHA patients in the Master Veteran Index (MVI), regardless of where a patient is registered for care, or if a

patient received treatment or benefits. As defined by VHA Handbook 1907.01 Health Information Management and Health Records, the Master Veteran Index (MVI) is a VA enterprise-wise system that uniquely identifies all active patients who have been admitted, treated, or registered in any VA medical facility.

h. **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.*

i. **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, biometric records, etc. 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, mother's maiden name, etc. Information does not have to be retrieved by any specific individual or unique identifier (i.e., covered by the Privacy Act) to be personally identifiable information.

j. **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.*

k. **Special User**. A special user is:

(1) An individual permitted access at a national level 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) A non-clinical user who requires specialized access to VHA PII or PHI in VHA managed IT systems for assigned purposes, such as broad access to electronic health records beyond the local level (e.g., national level access to Compensation and Pension Record Interchange (CAPRI) or Veterans Health Information Systems and Technology Architecture Web (VistAWeb)) or at a very discreet, highly-controlled individual patient level.

(3) Special users are managed at a national level by the VHA National Data Systems (NDS), Health Information Access (HIA) Program. ***NOTE:*** *Local access provided at the local level is not considered special user access.*

(4) A special user may be, but is not necessarily, a VA employee. Special users may include, but are not limited to contract staff, the VHA Office of Quality and Safety, OGC, VA Office of the Inspector General (OIG), DoD, Veterans Benefits Administration, Veteran Service Officers, and Office of Community Care.

l. **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.

4. POLICY

It is VHA policy that only individuals who are appropriately approved and meet all VA and VHA policy requirements will be granted access to VHA data processed and stored on VA IT systems. ***NOTE:*** *This directive does not negate any existing authority permitting a VA or VHA program office to use or obtain VHA data (Sensitive Personal Information (SPI), Individually Identifiable Information (III), PII, PHI or Electronic Protected Health Information (ePHI)).* This directive and corresponding VHA Handbook 1080.01, only outline the policy and process requirements for granting access to VHA data in VA IT systems. This policy does not encompass VHA PII contained in medical devices or on paper.

5. RESPONSIBILITIES

a. **Assistant Deputy Under Secretary for Health for Informatics and Information Governance.** The Assistant Deputy Under Secretary for Health for Informatics and Information Governance (OIIG) 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 ensure effective management of 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 are adopted which establish VHA-wide requirements to authorize access to VHA PII in VA IT systems in accordance with Federal laws, regulations, and VA and VHA policies.

c. **Director, Health Care Security Requirements.** The Director, Health Care Security Requirements (HCSR) is responsible for ensuring data sharing agreements for use of VHA PII contained in VA IT systems with entities outside VHA, or internally as required by VHA policy, comply with VA and VHA policies, Federal laws and regulations.

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

(1) Establishing and maintaining VHA-wide requirements for managing 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 apply the following criteria before granting a requestor access to VHA PII; the Deputy Director, NDS ensures verification of the following:

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

(b) The requestor has completed VHA privacy training, if applicable, in accordance with VHA Directive 1605, VHA Privacy Program.

(c) The requestor has completed applicable VA information security training, including the completion of the National Rules of Behavior, in accordance with VA Directive 6500.

(d) 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.

(e) Data requests from entities outside VHA meet VHA privacy and security criteria and comply with applicable legal privacy authority for the disclosure.

(f) Data requests from VA researchers meet VHA privacy criteria, when a privacy review is required by VA or VHA policy.

(3) Establishing policy and procedures for auditing requestors' access on an ongoing basis to ensure compliance with VA and VHA policy, and conducting such audits, as needed.

(4) Establishing formal processes for VHA data owners to ensure requestors have access to VHA PII in VA IT systems.

(5) Approving, establishing and/or managing access to VHA PII through CAPRI, the VistAWeb and/or other VHA managed IT systems for special users.

e. **Veterans Integrated Service Network (VISN) and VA Medical Facility Directors.** 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 access only the minimum necessary VHA PII to perform their official duties based on assigned functional categories.

(3) Approving processes for clinical staff and clinical support staff.

(4) Approving, establishing and/or managing access to VHA PII for clinical staff and clinical support staff by verifying that:

(a) The requestor is a VA employee in the functional role of clinician or clinical support staff.

(b) The requestor requires access to VHA PII and/or PHI at the local VA medical facility or VISN level.

(c) The requestor has legal privacy authority to access VHA PII under Federal law and regulation, as well as VA and VHA policies.

(d) The requestor has completed VHA privacy and HIPAA-focused training, if applicable, in accordance with VHA Directive 1605.

(e) The requestor has completed applicable VA information security training, including the completion of the National Rules of Behavior, in accordance with VA Directive 6500.

(f) Coordinating with OI&T to ensure that the VA IT system to which the requestor will be accessing has advanced transactional auditing and access control capabilities.

(5) Auditing user access on an ongoing basis to ensure compliance with VA and VHA policy.

(6) Ensuring appropriate action is taken to resolve privacy and security incidents of unauthorized access detected through audits.

f. **Clinical Staff and Clinical Support Staff.** Clinical staff and clinical support staff are responsible for:

(1) Ensuring that national-level 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 involving VHA data resulting from access to VHA PII in VA IT systems in accordance with VHA and VA policy and the National Rules of Behavior.

(3) Completing the annual VHA HIPAA and VA Privacy and security training and awareness courses as required.

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 the VHA data owner if access to VHA PII is no longer needed, i.e., the Special User's official job duties change.

(3) Notifying VHA NDS if access to VHA PII through CAPRI or VistAWeb is no longer needed, i.e. the special user's official job duties change.

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

6. REFERENCES

These references contain all the requirements for users:

a. 38 U.S.C. § 7332.

b. 38 U.S.C. §§ 5721 et seq.

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

d. 38 CFR. 14.626-14.637.

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.

n. Department of Veterans Affairs FY 2014-2020 Strategic Plan.

o. National Defense Authorization Act of 2014, Public Law 113-66.

p. VA National Rules of Behavior VA Handbook 6500, Appendix G.