ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION IN NATIONAL VA DATA SYSTEMS

1. SUMMARY OF MAJOR CHANGES: This directive:

a. Amendment dated May 14, 2024:

(1) Updates directive title to Access to Personally Identifiable Information in National VA Data Systems.

(2) Updates references from VHA Directive 1605, VHA Privacy Program, dated September 1, 2019, to VHA Directive 1605.01, Privacy and Release of Information, dated July 24, 2023.

(3) Adds references to VHA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, dated June 30, 2023, and VHA Directive 1605.01.

(4) Removes responsibility for the VA medical facility Director to manage and review access to VHA PII for clinical staff and clinical support staff by verifying the criteria.

(5) Updates link for the Privacy Security and Events Tracking System (PSETS).

(6) Updates definitions for Personally Identifiable Information and Protected Health Information to match VHA Directive 1605.01.

(7) Updates Privacy Officers and Information System Security Officers responsibilities.

b. Directive as published September 28, 2023:

(1) Updates responsibilities for Chief Informatics Officer, Veterans Health Administration (VHA); Director, National Data Systems; Deputy Director, National Data Systems; Veterans Integrated Services Network Director, Department of Veterans Affairs (VA) medical facility Director, special users and clinical staff and clinical support staff (see paragraph 2).

(2) States VHA personally identifiable information verification criteria (see paragraph 3).

(3) States requirements for clinical staff, clinical support staff and special users to access VA information technology systems (see paragraph 4).

2. RELATED ISSUES: VHA Directive 1080.01(1), Data Use Agreements, dated January 19, 2021.

3. POLICY OWNER: The Director, National Data Systems (105HIG) is responsible for the content of this directive. Questions may be referred to the Deputy Director, National Data Systems at VHAHIGHIA@va.gov.

4. RESCISSIONS: VHA Directive 1080, Access to Personally Identifiable Information in Information Technology Systems, dated January 6, 2017, is rescinded.

5. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last working day of September 2028. This VHA directive will continue to serve as national VHA policy until it is recertified or rescinded.

6. IMPLEMENTATION SCHEDULE: This directive is effective upon publication.

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

/s/ Steven Lieberman, MD, MBA
Deputy Under Secretary for Health

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 November 7, 2023.

CONTENTS

ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION IN NATIONAL VA DATA SYSTEMS

ACCESS TO PERSONALLY IDENTIFIABLE INFORMATION IN NATIONAL VA DATA SYSTEMS

1. POLICY

It is Veterans Health Administration (VHA) policy that only approved individuals who meet all Department of Veterans Affairs (VA) and VHA policy requirements are granted access to Personally Identifiable Information (PII), including protected health information (PHI), processed and stored on VA Information Technology (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, Individually Identifiable Information, PII, PHI or Electronic Protected Health Information (ePHI)). This directive does not apply to VHA PII or PHI contained in medical devices or on paper*.
AUTHORITY: 5 U.S.C. § 552a(e)(10); 45 C.F.R. Parts 160 and 164.

2. 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.** The Deputy Under Secretary for Health is responsible for supporting National Data Systems (NDS) with implementation and oversight of this directive.

c. **Assistant Under Secretary for Health for Operations.** The Assistant Under Secretary for Health for Operations is responsible for:

(1) Communicating the contents of this directive to each of the Veterans Integrated Services Networks (VISNs).

(2) Assisting VISN Directors to resolve implementation and compliance challenges in all VA medical facilities within that VISN.

(3) Providing oversight of VISNs to ensure compliance with this directive and its effectiveness.

d. **Chief Informatics Officer, Veterans Health Administration.** The Chief Informatics Officer, VHA is responsible for:

(1) Providing sufficient resources to maintain an oversight function to ensure effective management of access to VHA information.

(2) Ensuring that VA staff and patients receive timely, relevant informatics products and resources, continuously improving Veterans' health.

e. **Executive Director, Health Information Governance.** The Executive Director, Health Information Governance is responsible for:

(1) Compliance monitoring and managing national data systems.

(2) Developing and implementing policy and regulations in accordance with the Freedom of Information Act, Privacy Act, Title 38 confidentiality statutes and Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

f. **Director, National Data Systems.** The Director, NDS is responsible for:

(1) Overseeing VISN and VA medical facility compliance with this directive and ensuring corrective action is taken when non-compliance is identified.

(2) Establishing and maintaining VHA-wide requirements for managing access to VHA PII and PHI in VA IT systems in accordance with Federal statutes, regulations and VA and VHA policies. ***NOTE:*** *For more information see VHA Directive 1605.02, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information, dated April 4, 2019.*

(3) Establishing and distributing policies and procedures to authorize access to VHA PII and PHI in VA IT systems.

(4) Ensuring verification of the criteria to access VHA PII and PHI (see paragraph 3).

(5) Ensuring that the Deputy Director, NDS administers the Health Information Access (HIA) Program.

(6) Ensuring that policies and procedures are adopted which establish VHA-wide requirements to authorize access to VHA PII and PHI in VA IT systems in accordance with Federal laws, regulations and VA and VHA policies.

(7) Managing, tracking, and approving authorization for clinical staff, clinical support staff and special user access to VHA health information resources and national data systems comprising of PHI and other sensitive PII and PHI contained in clinical and administrative systems.

(8) Ensuring that all access to VHA PII and PHI in VA IT systems adheres to VA's data ethics standards regarding access to and use of Veterans health data, in accordance with 38 C.F.R. § 0.605. ***NOTE:*** *Questions about whether the ethical principles for data access and use are being met should be referred to the VA Data Governance Council's Data Ethics Workgroup or the VHA National Center for Ethics in Health Care.*

g. **Deputy Director, National Data Systems.** The Deputy Director, NDS is responsible for:

(1) Overseeing the provisioning of PII and PHI access to multiple data sources for operational and research purposes. ***NOTE:*** *See paragraph 3 for verification criteria.*

(2) Using established procedures, in accordance with VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, dated February 24, 2021; and VHA Directive 1605.01, Privacy and Release of Information, dated July 24, 2023, for auditing requestors' access on an ongoing basis to ensure compliance with VA and VHA policy, and conducting such audits, as needed.

(3) Establishing formal processes for VHA data owners to ensure requestors have access national data.

(4) Approving, establishing, and managing access to VHA PII and PHI through Compensation and Pension Record Interchange (CAPRI), Joint Longitudinal Viewer (JLV) and other VHA managed IT systems for special users. ***NOTE:*** *For more information see the NDS Healthcare Operations Request Process at http://vaww.vhadataportal.med.va.gov/DataAccess/HealthcareOperationsRequestProcess.aspx. This is an internal VA website that is not available to the public.*

(5) Administering the HIA Program.

h. **Director, Health Care Security.** The Director, Health Care Security is responsible for ensuring that data sharing agreements with VHA and non-VHA entities for use of VHA PII and PHI in VA IT systems comply with VA and VHA policies, Federal laws and regulations related to information security.

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

(1) Ensuring that all VA medical facilities within the VISN comply with this directive and informing leadership when barriers to compliance are identified.

(2) Ensuring access is granted in accordance with this directive, VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, dated June 30, 2023, and VHA Directive 1605.01.

(3) Ensuring that all staff at VA medical facilities within the VISN access only the minimum necessary data to perform their official duties based on assigned functional categories.

(4) Ensuring that all access adheres to VA's data ethics standards regarding access and use of Veterans' health data in accordance with 38 C.F.R. § 0.605. ***NOTE:*** *Questions about whether the ethical principles for data access and use are being met should be referred to the VA Data Governance Council's Data Ethics Workgroup or the VA National Center for Ethics in Health Care.*

j. **VA Medical Facility Director.** The VA medical facility Director is responsible for:

(1) Ensuring overall VA medical facility compliance with this directive and that appropriate corrective action is taken if non-compliance is identified.

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

(3) Appointing a VA medical facility management official to oversee access to PHI and PII for systems outside of VA Office of Information Technology (OIT) administration, including Software as a Service (SaaS), SharePoint sites and legacy systems in Austin Technology Center when the access process does not go through OIT.

(4) Ensuring that appropriate action to address privacy and security incidents is taken by clinical staff and support staff, in collaboration with Privacy Officers and Information System Security Officers, to ensure compliance with VA and VHA policy.

k. **VA Medical Facility Clinical Staff and Clinical Support Staff.** VA medical facility clinical staff and clinical support staff are responsible for:

(1) Ensuring that national-level access 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 of inappropriate access to the VA medical facility Privacy Officers and Information System Security Officers for inclusion into the Privacy Security and Events Tracking System (PSETS), in accordance with VA Handbook 6500.2. ***NOTE:*** *PSETS is the VA-wide system for documenting and tracking privacy and security events located at https://yourit.va.gov/now/nav/ui/classic/params/target/$pa_dashboard.do?eb41d2d01b312550205f5316624bcb70. This is an internal VA website that is not available to the public.*

(3) Completing the annual training courses as required by VA Handbook 6500.2 and VHA Directive 1605.01 prior to obtaining national-level access.

(4) Reporting any security or privacy incident that also poses a risk to patient safety in the Joint Patient Safety Reporting System (JPSR) as outlined in VHA Directive 1050.01, VHA Quality and Patient Safety Programs, dated March 24, 2023.

l. **Special Users.** Special users as identified in paragraph 4 are responsible for:

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

(2) Ensuring that all access adheres to VA's data ethics standards regarding access to and use of Veterans' health data in accordance with 38 C.F.R. § 0.605. ***NOTE:*** *Questions about whether the ethical principles for data access and use are being met should be referred to the VA Data Governance Council's Data Ethics Workgroup or the VA National Center for Ethics in Health Care.*

(3) Notifying the VHA data owner if access is no longer needed (i.e., the special user's official job duties change).

(4) Notifying the Deputy Director, NDS if access through CAPRI or JLV is no longer needed (i.e., the special user's official job duties change).

(5) Reporting any security or privacy incident that also poses a risk to patient safety in the Joint Patient Safety Reporting System (JPSR) as outlined in VHA Directive 1050.01.

(6) Reporting any security or privacy incidents involving inappropriate access to designated Privacy Officers and Information System Security Officers for inclusion into PSETS in accordance with VA Handbook 6500.2 and VHA Directive 1605.01.

m. **Privacy Officers and Information System Security Officers.** Privacy Officers and Information System Security Officers are assigned at both VISN and VA medical facilities and are responsible for:

(1) Entering complaints into PSETS and performing fact-findings of inappropriate access to VA IT systems involving PII and PHI, in accordance with VA Handbook 6500.2 and VHA Directive 1605.01.

(2) Monitoring mandatory privacy and security training of VA staff as specified in VA Handbook 6500.2 and VHA Directive 1605.01 for obtaining national-level access.

3. VHA PERSONALLY IDENTIFIABLE INFORMATION VERIFICATION CRITERIA

a. Prior to granted access, the Deputy Director, NDS must ensure verification of the following:

(1) The requestor has legal authority to access VHA PII and PHI under applicable Federal laws, regulations and VA and VHA policies.

(2) The requestor has completed mandatory training, in accordance with VA Handbook 6500.2 and VHA Directive 1605.01.

(3) 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 Directive 1605.01.

(4) Purpose for access is for treatment, payment, health care operations, or approved VA human subjects research in accordance with applicable federal laws, regulations, VA and VHA policies.

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

(6) PII and PHI requests from VA researchers meet VHA privacy criteria, when a research privacy compliance review is required by VA or VHA policy.

b. The VA medical facility Director ensures verification of the following:

(1) The requestor requires access to VHA PII or PHI at the VA medical facility or VISN level.

(2) The requestor has legal authority to access VHA PII and PHI under applicable Federal laws, regulations and VA and VHA policies.

c. Upon delegation from the VA medical facility Director, Information System Security Officers ensure that the requestor has completed applicable VA information security training, including the completion of the National Rules of Behavior, in accordance with VA Directive 6500.2.

d. Upon delegation from the VA medical facility Director, Privacy Officers ensure that the requestor has completed VHA privacy and HIPAA-focused training in accordance with VHA Directive 1605.01.

4. REQUIREMENTS FOR CLINICAL STAFF, CLINICAL SUPPORT STAFF AND SPECIAL USERS TO ACCESS NATIONAL VA IT SYSTEMS

a. The following are clinical staff and clinical support staff who can access VHA PII and PHI:

(1) An individual permitted by Federal statute or regulation and -

(a) VA to have access to one or more VA IT systems; or

(b) VHA, in accordance with all applicable VHA policy and with a need to know related to treatment, payment or health care operations, and approved VA human subjects research to have access to VHA PII or PHI.

(2) An individual is permitted national-level access to VHA PII and PHI 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. VA personnel includes VA employees, without compensation clinicians and Health Professions Trainees.

b. Special users are managed at a national level by Deputy Director, NDS. ***NOTE:*** *Local access provided at the VA medical facility level is not considered special user access.* A special user may be, but is not necessarily, a VA employee. Special users may include, but are not limited to contract staff, the Office of Quality and Patient

Safety, Office of General Counsel (OGC), VA Office of the Inspector General, VHA Clinical Services program offices, Department of Defense, Veterans Benefits Administration, Veteran Service Organizations and Office of Integrated Veteran Care. The following are special users who can access VHA PII and PHI:

(1) An individual permitted national-level access by:

(a) Federal statute or regulation to have access to or obtain a copy of VHA PII or PHI;

(b) 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 CAPRI and JLV or at a very discreet, highly controlled individual patient level).

5. TRAINING

The following training is ***required*** for users who wish to request access as stipulated in paragraph 4:

a. For clinical staff: VA 20152, Mandatory Training for Transitory, Part-time and Intermittent Clinical Staff (MTTCS).

b. For Health Professions Trainees: VA 3185966, VHA Mandatory Training for Trainees and VA 3192008, VHA Mandatory Training for Trainees – Refresher.

c. For all VA medical facility staff: VA 10203, Privacy and HIPAA Training and VA 10176, VA Privacy and Information Security Awareness and Rules of Behavior (WBT).

6. RECORDS MANAGEMENT

All records regardless of format (for example, paper, electronic, electronic systems) created by this directive must be managed as required by the National Archives and Records Administration (NARA) approved records schedules found in VHA Records Control Schedule 10-1. Questions regarding any aspect of records management can be addressed to the appropriate Records Officer.

7. BACKGROUND

a. The Privacy Act of 1974 (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 and PHI that is stored electronically.

b. HIPAA (P.L. 104-191) and its implementing regulations (45 C.F.R. Parts 160 and 164) include requirements to ensure the security and privacy of PHI and PII 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 Health Information Technology for Economic and Clinical Health Omnibus Rule of January 23, 2013) apply to all PHI and PII 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 and PII.

8. DEFINITIONS

a. **Access.** Access is the ability to view, inspect or obtain a copy of VHA PII or PHI electronically, on paper or through another medium, for the purpose of performing an official function.

b. **Access Control.** Access control is an IT system capability that automatically creates a continuous record of user system actions and provides the ability to restrict individual user access.

c. **Clinical Staff.** For the purposes of this directive, clinical staff are VA health care providers in occupations which have qualification standards which require licensure, certification or registration in order to provide direct patient care. Examples include but are not limited to physicians, dentists, registered nurses, social workers and dietitians.

d. **Clinical Support Staff.** For the purposes of this directive, clinical support staff are individuals in occupations that support patient care with work which does not provide direct diagnosis, treatment or care for the patient and that is documented in a patient record. For example, medical record technicians, medical supply technicians or medical support assistants.

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 is also an agency official who has been identified as having the responsibility and the accountability for the use or disclosure of the PII and PHI contained in a VA IT system. These responsibilities may extend to interconnected systems or groups of interconnected systems. As determined by OGC, the official owner of PII and PHI within VHA is the Under Secretary for Health. ***NOTE:*** *It is VHA practice to delegate responsibility and accountability for business functions and the PII 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 PII and PHI.*

f. **Electronic Protected Health Information.** Under the HIPAA Privacy Rule, ePHI is any individually identifiable health information PHI 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 information that 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 does not include employment records held by VHA in its role as an employer.*

g. **Joint Longitudinal Viewer.** The JLV is health data viewer that has been implemented by VA to meet its interoperability requirements. JLV provides an integrated, standardized view of health records from all sites and systems where a patient has received care in VA, Department of Defense and from community partners, helping providers see an entire patient's medical history, thus enabling better informed care decisions. JLV is used in all VA medical facilities nationwide as well as all Veterans Benefits Administration sites and is being used by more than 115,000 individuals, helping to connect patient information between multiple VA health care providers and civilian providers where applicable.

h. **National-Level Access.** National-level access is access to health records of all VHA patients in the Master Person Index (MPI), regardless of where a patient is registered for care or whether a patient received treatment or benefits. ***NOTE:*** *As defined by VHA Directive 1906, Data Quality Requirements for Health Care Identity Management and Master Person Index Functions, dated April 10, 2020, the MPI is the authoritative identification service within VA for establishing, maintaining and synchronizing identities for VA persons, (e.g., Veterans, beneficiaries, patients, employees, IT users and VA health care providers).*

i. **Need to Know.** Need to know is the requirement of a VHA health care employee to obtain access to or possess PHI that is needed to carry out official job duties in relation to treatment, payment, or health care operations. Need to know is considered the same as a required business need. See VHA Directive 1605.02.

j. **Personally Identifiable Information.** PII is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples of PII elements include but not limited to: name, social security number (SSN) and 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. ***NOTE:*** *The term "Personally Identifiable Information" is synonymous and interchangeable with "Sensitive Personal Information". PII may not be protected by the Privacy Act if it is not required to be retrieved by name or unique identifier. For data definitions and relationships, see VHA Directive 1605.01 Appendix C*.

k. **Protected Health Information.** For purposes of this directive, PHI is individually identifiable health information transmitted or maintained in any form or medium by a

covered entity, such as VHA. ***NOTE:*** *VHA uses the term PHI to include information that is covered by HIPAA but unlike PII, may or may not be covered by the Privacy Act or title 38 confidentiality statutes. PHI excludes employment records held by VHA in its role as an employer, even if those records include information about the health of the employee obtained by VHA in the course of employment of the individual. VHA Directive 1605.01, Appendix C shows the relationship between the various data definitions.*

l. **Transactional Auditing.** Transactional auditing is an IT system capability that automatically creates a continuous record of user system actions and provides the ability to restrict individual user access.

m. **VA Information Technology Systems.** 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.

9. REFERENCES

a. P.L. 104-191.

b. 5 U.S.C. § 552a.

c. 38 C.F.R. § 0.605.

d. 45 C.F.R. Parts 160 and 164.

e. VA Directive 6500, VA Cybersecurity Program, dated February 24, 2021.

f. VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, dated February 24, 2021.

g. VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, dated June 30, 2023.

h. VHA Directive 1050.01, VHA Quality and Patient Safety Programs, dated March 24, 2023.

i. VHA Directive 1605.01, Privacy and Release of Information, dated July 24, 2023.

j. VHA Directive 1605.02, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information, dated April 4, 2019.

k. VHA Directive 1906, Data Quality Requirements for Health Care Identification Management and Master Person Index Functions, dated April 10, 2020.

l. NDS Healthcare Operations Request Process. http://vaww.vhadataportal.med.va.gov/DataAccess/HealthcareOperationsRequestProcess.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

m. ServiceNow (formerly PSETS). https://yourit.va.gov/now/nav/ui/classic/params/target/$pa_dashboard.do?eb41d2d01b312550205f5316624bcb70. ***NOTE:*** *This is an internal VA website that is not available to the public.*