PRIVACY AND RELEASE OF INFORMATION

1. SUMMARY OF MAJOR CHANGES: This directive revises, consolidates and updates procedures involving privacy and the release of information, and includes the following major changes:

a. Adds responsibilities for Department of Veterans Affairs (VA) staff (see paragraph 2).

b. Updates definitions in paragraph 41, including personally identifiable information and VA health care facility. ***NOTE:*** *VA health care facility (i.e., Facility) and VA medical facility have different definitions with specific and intentional uses within this directive.*

c. Adds Appendix C on Data Relationships.

d. Adds information on Agency Accounting of Disclosures (see paragraph 37), Written Requests (see paragraphs 3, 14, 21 and 27) and Information Blocking (see paragraph 15).

e. Adds information under public health authorities for Centers for Disease Control and Prevention and public health crises (see paragraph 27).

f. Updates information on the Health Information Exchange (see paragraphs 24 and 36).

g. Makes clarifications based on the MISSION Act updates to 38 U.S.C. § 7332 and emerging issues due to implementation of VA's new electronic health record.

2. RELATED ISSUES: VA Directive 6213, Freedom of Information Act (FOIA), dated September 15, 2021; VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, dated August 19, 2013; VA Handbook 6300.5, Procedures for Establishing and Maintaining Privacy Act Systems of Records, dated August 3, 2017; VA Handbook 6300.6, Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses, dated October 21, 2015; as well as Veterans Health Administration (VHA) directives included in the 1605 series.

3. POLICY OWNER: VHA Office of Health Informatics, Information Access and Privacy (105HIG) is responsible for the content of this directive. Questions may be referred to the VHA Chief Privacy Officer at VHAPrivIssues@va.gov.

4. RESCISSION: VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016, is rescinded.

5. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last working day of July 2028.

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

BY THE 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 July 25, 2023.

CONTENTS

PRIVACY AND RELEASE OF INFORMATION

PRIVACY AND RELEASE OF INFORMATION

1. POLICY

It is Veterans Health Administration (VHA) policy to conform to the legal requirements for collecting, using and disclosing personally identifiable information, including protected health information (PHI), and the appropriate handling of individuals' privacy rights regarding personally identifiable information based on the analysis of all applicable Federal privacy laws and regulations, resolving conflicts in favor of applying the most stringent requirements. This directive must be used as a reference tool for documenting and facilitating the appropriate use and disclosure of information maintained by VHA. **AUTHORITY:** 5 U.S.C. § 552a, 38 U.S.C. §§ 5701, 5705, 7301(b), 7332; 38 C.F.R. §§ 1.460-1.582, 17.500-17.511; 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 the VHA Information Access and Privacy (IAP) Office 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) Ensuring that Veterans Integrated Services Network (VISN) Directors implement privacy programs within their VISN.

(2) Assisting VISN Directors to resolve privacy program implementation and compliance challenges in all Department of Veterans Affairs (VA) medical facilities within that VISN.

(3) Communicating the contents of this directive to each of the VISNs.

(4) Providing oversight of VISNs to ensure compliance with this directive and its effectiveness, including organizational alignment of Privacy Officers.

d. **Chief Informatics Officer.** The Chief Informatics Officer is responsible for:

(1) Ensuring that IAP implements VHA-wide privacy policies and procedures defined in this directive through the VHA Privacy Program. ***NOTE:*** *See VHA Directive 1605, VHA Privacy Program, dated September 1, 2017, for further information.*

(2) Ensuring the VHA Privacy Program mission and vision are accomplished by supporting resources, funding and staffing.

e. **Director, Information Access and Privacy/VHA Chief Privacy Officer.** The Director, IAP/VHA Chief Privacy Officer is responsible for:

(1) Issuing VHA-wide privacy policies and procedures for implementation of the national VHA Privacy Program in accordance with VHA Directive 1605 and this directive.

(2) Developing, issuing, reviewing and coordinating privacy policy for VHA in conjunction with policy efforts by VA.

(3) Issuing direction to the VHA Privacy Operations Officer, Facility Privacy Officers and VHA program office Privacy Liaisons regarding all aspects of implementing the VHA Privacy Program.

(4) Providing VHA program offices with privacy guidance on any Memorandums of Understanding/Agreement (MOU/MOA) or Data Use Agreement (DUA) requirements when the VHA program office plans to share personally identifiable information with an outside entity.

(5) Providing VHA-specific privacy training tools for compliance with the annual training requirement and this directive (see paragraph 38).

(6) Establishing VHA policy on the reporting, tracking, investigation and resolution of VHA privacy complaints and incidents through this directive and the Guide to Investigating Privacy Events in VHA, available at: https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/FactSheets.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

(7) Communicating deficiencies by VA medical facilities in privacy complaint or incident response to VISN Privacy Officers.

(8) Delegating, as appropriate, any of the duties outlined in this directive to designated employees within IAP.

f. **VHA Chief Program Officers.** VHA Chief Program Officers are responsible for:

(1) Ensuring compliance within VHA program offices with all internal and external requirements including Federal statutes and regulations, VA regulations and policies and VHA policies relating to privacy.

(2) Ensuring policies and procedures are consistent with standards contained in this directive within their respective programs and distributed to all personnel.

(3) Consulting with the VHA Privacy Office within IAP prior to any new collection or creation of personally identifiable information to ensure Privacy Act Systems of Records requirements are addressed in accordance with VA Handbook 6300.5, Procedures for Establishing and Maintaining Privacy Act Systems of Records, dated August 3, 2017.

(4) Ensuring all personnel within VHA program offices complete privacy training in accordance with VHA privacy policy before they are granted access to any personally identifiable information and that personnel complete the privacy training annually (see paragraph 38).

(5) Designating an individual with privacy experience which may include certification, such as Certified Information Privacy Professional (CIPP), to serve as the VHA program office Privacy Officer or Liaison, as appropriate, to provide guidance and oversight to ensure compliance with privacy regulations for their respective programs.

(6) Ensuring VHA program offices under their purview have appropriate privacy expertise and coverage at all levels to ensure compliance with this directive.

g. **VHA Privacy Operations Officer.** The VHA Privacy Operations Officer is responsible for:

(1) Managing the VHA Privacy Office and implementing the VHA Privacy Program as directed by the VHA Chief Privacy Officer.

(2) Implementing approved VHA-wide privacy policies and procedures through the VHA Privacy Office.

(3) Establishing requirements for the responsibilities of VISN and VA medical facility Privacy Officers and VHA program office Privacy Liaisons and providing implementation guidance, as needed.

(4) Providing all training on VHA-wide privacy policies to Facility Privacy Officers.

(5) Ensuring VISN and VA medical facility Privacy Officers are aware of the process for recording all actual or suspected incidents of privacy observed or reported in the tracking system designated by the VA Data Breach Resolution Service (e.g., Privacy and Security Event Tracking System (PSETS)).

(6) Ensuring Facility Privacy Officers respond to privacy incidents and complaints within the required timeframe prescribed by VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, dated June 30, 2023.

(7) Responding to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) on all Health Insurance Portability and Accountability Act (HIPAA)-related privacy and security complaints received within VHA.

h. **Veterans Integrated Service Network Directors.** VISN Directors are responsible for:

(1) Ensuring compliance within their respective facilities and programs with all internal and external requirements including Federal statutes and regulations, VA regulations and policies and VHA policies relating to privacy.

(2) Ensuring privacy programs, policies and procedures are consistent with standards contained in this directive within their respective programs and distributed to all personnel.

(3) Consulting with the VHA Privacy Office prior to any new collection or creation of personally identifiable information to ensure Privacy Act Systems of Records requirements are addressed in accordance with VA Handbook 6300.5.

(4) Ensuring that all personnel within their respective facilities complete privacy training in accordance with VHA privacy policy before they are granted access to any personally identifiable information and that personnel complete the privacy training annually (see paragraph 38).

(5) Designating an individual with privacy experience which may include certification, such as CIPP, to serve as the VISN Privacy Officer, as appropriate, to provide guidance and oversight to ensure compliance with privacy regulations for their respective programs.

(6) Ensuring the VISN cooperates with and responds to requests from VHA IAP within the timeframes set by IAP to meet statutory and regulatory requirements.

(7) Ensuring facilities and programs under their purview have appropriate privacy expertise and coverage at all levels to ensure compliance with this directive.

i. **VHA Program Office Privacy Officer or Liaison.** The VHA program office Privacy Officer or Liaison is responsible for:

(1) Developing VHA program office privacy practices consistent with this directive.

(2) Providing guidance to the VHA program office on all privacy-related matters such as the Privacy Act, Freedom of Information Act (FOIA), HIPAA Privacy Rule and title 38 United States Code confidentiality statutes; and seeking guidance and advice from the VHA Chief Privacy Officer to resolve any questions or concerns about privacy-related issues.

(3) Ensuring all complaints, incidents and actual or suspected breaches of privacy by the VHA program office and associated facilities (e.g., Vet Centers), are reported and recorded (by the Privacy Officer, Privacy Liaison or other responsible party, as appropriate to the circumstances) in the system designated by the VA Data Breach Resolution Service (e.g., PSETS) and in accordance with VA Handbook 6500.2.

(4) Ensuring the VHA program office responds to requests from the VHA Chief Privacy Officer or designee for information on complaints, incidents and actual or suspected breaches of privacy for timely resolution in accordance with this directive (see paragraph 37.c.).

(5) Ensuring the VHA program office and any associated facilities (e.g., Vet Centers) comply with all corresponding privacy standards associated with this directive.

(6) Coordinating with VHA Chief Privacy Officer or designee on any MOU/MOA or DUA when sharing personally identifiable information with an outside entity.

(7) Tracking privacy training annually and reporting the compliance to the VHA Chief Privacy Officer, upon request.

j. **Veterans Integrated Service Network Privacy Officer.** The VISN Privacy Officer is responsible for:

(1) Developing VISN privacy practices consistent with this directive.

(2) Providing expert privacy guidance to each VISN facility and VISN staff on all privacy-related matters such as the Privacy Act, FOIA, HIPAA Privacy Rule and title 38 United States Code confidentiality statutes and seeking guidance and advice from the VHA Privacy Office to resolve any questions or concerns about privacy-related issues.

(3) Ensuring the VISN office and all VA medical facilities within the VISN respond to requests from VHA Privacy Office by the deadline specified by the VHA Privacy Office.

(4) Ensuring all complaints, incidents and actual or suspected breaches of privacy within the VISN are reported (by the VISN Privacy Officer or other responsible party, as appropriate to the circumstances) in the system designated by the VA Data Breach Resolution Service (e.g., PSETS) and in accordance with VA Handbook 6500.2.

(5) Ensuring complaints, incidents and actual or suspected breaches of privacy by VISN staff are investigated and resolved.

(6) Ensuring a national Business Associate Agreement (BAA) is in place for VISN-level contracts or other agreements (e.g., MOU/Interconnection Security Agreement (ISA)) involving the disclosure of personally identifiable information to the contractor or other outside entity.

(7) Partnering with VA medical facility Privacy Officers within their VISN to ensure that they have the necessary resources, training and support to build a privacy program in accordance with VHA Directive 1605 and this directive.

(8) Obtaining VISN-wide standing written request letters from each State agency requesting patient data for public health reporting, law enforcement reporting or other State reporting mandate from the VA medical facilities in the VISN and sharing the VISN-wide standing written request letters with the VHA Privacy Office, as requested.

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

(1) Designating an individual with privacy experience which may include CIPP or other related experience, to serve as VA medical facility Privacy Officer as outlined in paragraph 37.a.

(2) Ensuring compliance within the VA medical facility with all Federal laws, regulations, VA regulation and policies and VHA policies relating to privacy.

(3) Ensuring VA medical facility policies and procedures are consistent with standards contained in this directive and are distributed to all employees.

(4) Ensuring all personnel within the VA medical facility obtain privacy training before they are granted access to any Veteran or patient personally identifiable information as required by VA Directive 6502, VA Enterprise Privacy Program, dated May 5, 2008, and that personnel receive the follow-up privacy training as required.

(5) Ensuring all personnel within the VA medical facility complete annual privacy training in accordance with applicable requirements and this directive as outlined in paragraph 38.

(6) Implementing the requirements of the VHA Privacy Program as it applies to VA medical facilities. See VHA Directive 1605 for further information.

(7) Ensuring all personnel within the VA medical facility are aware of their respective VA medical facility Privacy Officer and report any complaints, incidents and actual or suspected breaches of privacy to the VA medical facility Privacy Officer in accordance with VA Handbook 6500.2.

(8) Ensuring all complaints, incidents and actual or suspected breaches of privacy by the VA medical facility are recorded (by the Privacy Officer or other responsible party, as appropriate to the circumstances) in the tracking system designated by the VA Data Breach Resolution Service (e.g., PSETS) in accordance with VA Handbook 6500.2.

(9) Ensuring the VA medical facility Privacy Officer completes contract security reviews and local BAA for VA medical facility-level contracts, purchase orders or agreements where the vendor requires access to PHI in accordance with VHA Directive 1605.05, Business Associate Agreements, dated November 17, 2020.

(10) Signing notifications to individuals whose privacy rights of access or amendment requests are denied (see paragraphs 7.c. and 8).

l. **VA Medical Facility Privacy Officer.** The VA medical facility Privacy Officer is responsible for:

(1) Reporting activities of the VA medical facility Privacy Program and the policies outlined in this directive directly to the VA medical facility Director or Associate Director for privacy responsibilities as the designated VA medical facility Privacy Officer(s).

(2) Using the VA medical facility privacy policy template to develop facility privacy policies consistent with the VHA Privacy Program and this directive (see paragraphs 3.a. and 4.b. for additional information, including a link to the template).

(3) Providing expert guidance to the VA medical facility on all privacy-related matters, such as the Privacy Act, FOIA, HIPAA Privacy Rule and title 38 United States Code confidentiality statutes and seeking guidance and advice from their VISN Privacy Officer or the VHA Privacy Office to resolve any questions or concerns about privacy-related issues.

(4) Ensuring that the VA medical facility responds to requests from the VHA Privacy Office by the deadline as specified by the VHA Privacy Office.

(5) Ensuring that all complaints, incidents and actual or suspected breaches of privacy of personally identifiable information by the VA medical facility are reported to the tracking service designated by the VA Data Breach Resolution Service (e.g., PSETS) in accordance with VA Handbook 6500.2 and these complaints, incidents and actual or suspected breaches of privacy are investigated and resolved.

(6) Conducting privacy-related reviews, such as contract security reviews, BAAs, privacy presentation or publication reviews and research protocol privacy reviews, as required by VHA Directive 1605 prior to the use or disclosure of PHI.

(7) Reviewing the HIPAA authorization and requested waivers of HIPAA authorization to ensure legal authority exists prior to the use, access, collection, creation and disclosure of PHI (obtained orally or in writing) by research investigators.

(8) Reviewing any MOU/MOA, MOU/ISA or DUA when sharing or disclosing VA medical facility-level personally identifiable information with an outside entity.

(9) Ensuring, in conjunction with the VA medical facility Information Systems Security Officer (ISSO), that a process exists to flag patient records in the Veterans Health Information Systems and Technology Architecture (VistA) in accordance with this directive.

(10) Providing guidance to the VA medical facility Director on how the VA medical facility may comply with all corresponding VA or VHA privacy directives associated with this directive.

(11) Performing all privacy-related duties outlined in VHA Directive 1605 and VA Directive 6509, Duties of Privacy Officers, dated July 30, 2015.

m. **VA Personnel.** All VA personnel collecting, accessing, using, disclosing, sharing or storing VHA data regardless of Administration or Staff Office are responsible for:

(1) Complying with all Federal laws and regulations, VA regulations and policies, national VHA policies and local (VHA program office, VISN or VA medical facility) policies relating to the privacy of VHA data and this directive.

(2) Completing all applicable VA- and VHA-required privacy training at the time of employment, annually thereafter, and as directed when changes are made to update the required training.

(3) Knowing who is their respective Privacy Officer and reporting all complaints, incidents and actual or suspected breaches of privacy in a complete manner upon discovery to the Privacy Officer, according to established policy.

(4) Seeking guidance and advice from their respective Privacy Officer to resolve any questions or concerns about privacy-related issues regarding VHA data.

(5) Ensuring privacy authority exists, which may require consultation with an appropriate VHA privacy official, prior to collecting, accessing or using VHA data containing personally identifiable information or PHI within VA.

(6) Ensuring privacy authority exists, which may require consultation with an appropriate VHA privacy official, prior to sharing or disclosing personally identifiable information or PHI outside VA.

(7) Collecting, using, accessing, disclosing or requesting PHI from VHA only as necessary and to the minimum amount required to perform their specific job functions and when legal authority exists to permit such collection, use, access or disclosure.

(8) Consulting with the Privacy Officer prior to any new collection or creation of personally identifiable information to ensure Privacy Act Systems of Records requirements are addressed in accordance with VA Handbook 6300.5.

(9) Ensuring auditory privacy by exercising appropriate precautions and safeguards when discussing Veterans' personally identifiable information or PHI.

n. **VHA Employees.** All VHA employees, as defined in paragraph 41, are responsible for:

(1) Performing all of the responsibilities listed in paragraph 2.m. for VA personnel when collecting, accessing, using, disclosing, sharing or storing VHA data.

(2) Completing appropriate mandatory annual privacy training based on their position and access to VA information systems and VA data.

(3) Knowing who their respective Facility Privacy Officer is and reporting all complaints, incidents and actual or suspected breaches of privacy in a complete manner upon discovery to the Facility Privacy Officer, according to established policy.

3. COMPLIANCE WITH FEDERAL LAW, REGULATION AND VHA POLICY

a. **General Privacy Requirements.**

(1) All VHA employees are part of VHA as a health care provider and health plan under the HIPAA Privacy Rule regardless of their position. All VHA employees must comply with all Federal laws and regulations, regardless of their position; these include the HIPAA Privacy Rule, VA regulations and policies and VHA policies, including VHA Directive 1605.02, Minimum Necessary Standards for Access, Use, Disclosure and

Requests for Protected Health Information, dated April 4, 2019, which limits access to personally identifiable information based on position.

(2) All employees must conduct themselves in accordance with VA's national rules of conduct concerning the disclosure or misuse of information. Employees must annually sign the VA Information Security Rules of Behavior (formerly VA National Rules of Behavior) as required under 38 U.S.C. § 5723(f) and VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, dated February 24, 2021.

(3) All VA health care facilities must create facility policies that are consistent with the policies contained in this directive. VA medical facilities must use the VA Medical Center Privacy Policy Template to satisfy this requirement, available at: https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/templates.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

(4) This directive must be posted and available to all employees (e.g., posted on the VA health care facility's internal website).

(5) All employees who have access to VHA health or Veteran records must receive annual training on the requirements of Federal privacy and information laws and regulations, VA regulations and policies and VHA privacy policy. Training must also be provided at the time of VA employment and within 6 months of any significant change in Federal law, regulation, this directive or the VA health care facility's policies and procedures regarding privacy, and as otherwise directed in paragraph 38 of this directive.

(6) VA, including VHA, may not collect or maintain information about individuals that is retrieved by a name or personal identifier, as the records would be a Privacy Act System of Records, until a System of Records notice (SORN) is submitted for approval and may not disclose information collected about individuals until proper notifications are given to Congress and the Office of Management and Budget (OMB), and a SORN is published in the Federal Register as required by the Privacy Act.

(7) All VHA Privacy Act Systems of Records containing Veteran or patient health information are designated records sets under the HIPAA Privacy Rule. All individually identifiable information on Veterans and patients, including demographics, in Federal agency records in the possession of VHA is considered PHI. ***NOTE:*** *Psychotherapy notes are not Federal agency records owned by VHA as they are the personal session notes of the mental health professional.*

(8) All employee information maintained in the official Employee Medical Folder Privacy Act Systems of Records by VHA is PHI. Employee information maintained in the official Employee Medical Folder by VA at the Department level is not PHI.

b. **Use of Information.**

(1) All VHA employees may use information contained in VHA records required for the performance of their official job duties for treatment, payment or health care operations purposes. There must be an authorization or other legal authority (e.g., waiver of HIPAA authorization for research) in order to access a health record for any other reason. Browsing any health record for personal reasons such as looking up appointment for relatives or accessing the health record of or for a friend out of curiosity or at the request of the friend is strictly prohibited and is a privacy violation. These restrictions apply to supervisors the same as all other employees. In addition, supervisors cannot access employee records for employment or Human Resources (HR) purposes. Appropriate disciplinary action may be taken by an employee's supervisor with guidance from HR.

(2) All VHA employees must access or use only the minimum amount of information from VHA records necessary to fulfill or complete their official job duties in accordance with VHA Directive 1605.02.

(3) Where VHA has determined that it is legally permissible to provide access to and use information or data protected by one or more of the applicable confidentiality or privacy statutes or regulations, VHA may do so only after complying with the relevant legal requirements and considering VA's Ethics Principles for Access to and Use of Veteran Data (38 C.F.R. § 0.605).

(4) Sharing of personally identifiable information for official VA-approved research may require the completion of a DUA (see paragraph 13; VHA Directive 1080.01(1), Data Use Agreement, dated January 19, 2021; and VHA Handbook 1200.12, Use of Data and Data Repositories in VHA Research, dated March 9, 2009) or transmitting personally identifiable information externally for VA-approved research may require the completion of an MOU, DUA or other agreement (see VA Handbook 6500).

(5) VHA may use a limited data set for the purpose of public health, health care operations or research without obtaining a HIPAA authorization or waiver of HIPAA authorization. VHA may use individually identifiable health information to create a limited data set pursuant to a DUA. A limited data set is similar to de-identified information in that it has all direct patient identifiers removed, however, a limited data set may contain dates, State, city; and full five or nine-digit Zip codes.

(6) VHA records may be used for VA-approved research purposes as authorized by law.

(7) Information obtained by VA employees in the performance of official job duties must not be used for research purposes or publications without approval through appropriate VA authority in accordance with applicable VHA research policies including VHA Handbook 1200.12, 38 C.F.R. part 16 and this directive.

(8) The Office of General Counsel (OGC) Advisory Opinion (VAOGCADV 8-2004), Disclosure under the HIPAA Privacy Rule and the Privacy Act of Medical Records for

Use in an Employee Disciplinary Investigation, states that the Privacy Act does not allow the disclosure of a VHA employee's occupational health record or VHA employee's Veteran health record to management or personnel officials for disciplinary investigation purposes without prior written authorization from the employee. In addition, management or personnel officials, such as supervisors, may not access a VHA employee's occupational health record or VHA employee's Veteran health record for any other employment purpose without the prior written authorization from the employee. Appropriate disciplinary action of a management or personnel official who inappropriately accesses such records on employees may be taken by their supervisor with guidance from HR.

c. **Disclosure of Information.** ***NOTE:*** *Throughout this directive, various situations are described in which personally identifiable information may be disclosed. Because disclosure is discretionary, personally identifiable information must not be released unless it is determined that such disclosure is in the best interest of VA or the record subject (e.g., Veteran) except when disclosure is mandated by law or regulation. Questions regarding the appropriateness of such disclosure must be referred to the Facility Privacy Officer or the VHA Privacy Office in advance of the disclosure.*

(1) When VHA discloses personally identifiable information pursuant to legal authority other than a signed, written authorization, the disclosing VHA official must consider the applicability of VA's Ethics Principles for Access to and Use of Veteran Data (38 C.F.R. § 0.605). The disclosing VHA official must also notify the recipient, preferably in writing, that the information disclosed is confidential and the information must be handled with appropriate sensitivity. If VHA is retaining ownership of the information disclosed, the recipient must be made explicitly aware of this fact.

(2) Disclosure of information must be made only from official VHA records. When the request for disclosure requires copies of official VHA records, the request must be in writing. While some verbal disclosures may be made without a written request (e.g., to a health care provider for treatment), others will require a written request to satisfy disclosure authority (e.g., law enforcement officials for criminal investigation).

(3) Individually identifiable information from VHA records may be disclosed or released only upon receipt of the prior signed-written authorization of the individual or under other legal authority as outlined in this directive. All disclosures must be covered by or listed in the Information Bulletin (IB) 10-163, VHA Notice of Privacy Practices (see VHA Handbook 1605.04, Notice of Privacy Practices, dated October 7, 2015).

(4) Any individually identifiable information related to VHA treatment of drug abuse or referral for drug treatment, alcoholism or referral for alcohol treatment, sickle cell anemia, treatment for Human Immunodeficiency Virus (HIV) has special protection under 38 U.S.C. § 7332. The information can be disclosed only as authorized by 38 U.S.C. § 7332, VA implementing regulations at 38 C.F.R. §§ 1.460–1.496 and this directive.

(5) When disclosing personally identifiable information to non-governmental organizations or individuals, as authorized by law and this directive, for non-VA research purposes, VHA may condition the disclosure on the completion of a DUA, which specifies the conditions for the provision of the VHA data. ***NOTE:*** *For further discussion of the use of DUA for non-research purposes, see VHA Directive 1080.01(1)*.

(6) **Limited Data Sets.** VHA may disclose a limited data set for research, public health or health care operations pursuant to a DUA or MOU. The disclosure of a limited data set for public health does not have to be to a public health authority. See VHA Directive 1080.01(1).

(7) **De-identified Information.** VHA may disclose de-identified information for any purpose upon its own initiative or to another Federal agency. A request for de-identified information from a non-Federal entity must be processed under FOIA in accordance with VHA Directive 1935, VHA Freedom of Information Act Program, dated February 5, 2018.

d. **Sale of Protected Health Information.**

(1) VHA may not and does not sell PHI. VHA Business Associates may not sell PHI received from VHA.

(2) Except as otherwise described in paragraph 3.d.(3) below, the sale of PHI is a disclosure of PHI by a covered entity or Business Associate, if applicable, where the covered entity or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

(3) The following disclosures of PHI are not considered a sale of PHI:

(a) For public health purposes.

(b) For research purposes, where the only remuneration received by VHA or its Business Associate is a reasonable cost-based fee to cover the cost to prepare and transmit the PHI for such purposes.

(c) For treatment and payment purposes.

(d) To or by a Business Associate for activities that the Business Associate undertakes on behalf of VHA, or on behalf of a Business Associate in the case of a subcontractor, and the only remuneration provided is from VHA to the Business Associate or from the Business Associate to the subcontractor, if applicable, for the performance of such activities.

(e) To an individual, when requested under Right of Access or Accounting of Disclosures, and fees are charged for replication of the records.

(f) When required by law.

(g) For any other purpose permitted where the only remuneration received by VHA or its Business Associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose, or a fee otherwise expressly permitted by other law, such as FOIA fees.

e. **Fundraising.** VA health care facilities must not use Veterans' PHI for fundraising. If a VA health care facility believes they are using PHI for fundraising purposes, contact the VHA Privacy Office for additional guidance.

4. SAFEGUARDS

a. VHA, including each health care facility, must ensure that appropriate administrative, technical and physical safeguards are established to ensure the security and confidentiality of personally identifiable information and records, including PHI and to protect against any anticipated threats or hazards to the security or integrity of such records, which would result in substantial harm, embarrassment, inconvenience or unfairness to any individual about whom information is maintained. These safeguards require an employee to:

(1) Log off the computer or lock the computer screen when they walk away from the computer or at any time that the computer is left unattended.

(2) Secure and safeguard all PHI by locking it in a file cabinet or desk drawer. If an office is locked at all times and the only people with keys, including cleaning staff, have authority to see PHI, then PHI does not need to be in locked drawers. Be aware that contracted custodians never have authority to see PHI. PHI must not be left unattended, in accordance with VA Handbook 6500.

(3) Dispose of or destroy all documents containing PHI when no longer needed, in accordance with VA Directive 6371, Destruction of Temporary Paper Records, dated April 8, 2014, and all applicable records control schedules (RCS).

(4) Comply with the requirements contained in the VA Information Security Rules of Behavior (formerly VA National Rules of Behavior) found in the VA Privacy and Information Security Awareness and Rules of Behavior training.

b. Each VA medical facility must develop clear and explicit policies governing privacy requirements when employees are discussing sensitive patient care issues. Employees must be conscious of when and where it is appropriate to discuss issues involving individually identifiable health information to prevent identity theft or unauthorized disclosure of health information. For example, employees must:

(1) Speak quietly when discussing a patient's condition with family members in a waiting room, on the telephone or in other public areas.

(2) Speak quietly to the patient when in an open area (e.g., emergency room (ER) or multiple bed ward).

(3) Avoid speaking about patients' PHI in public hallways and elevators. Signs regarding principles of auditory privacy must be posted in public hallways and elevators to remind employees and others to protect patient confidentiality. ***NOTE:*** *Public hallways are areas for use by the public, such as the main entrance and corridors to the cafeteria and canteen. Hallways on inpatient wards or between clinic exam rooms are not public hallways. VA health care facilities do not have to build private, soundproof rooms or alter existing space to prevent overheard conversations about a patient's condition or health information. The HIPAA Privacy Rule simply requires that VA health care facilities provide reasonable safeguards to protect confidential information, such as using curtains, screens, white noise or similar barriers. If a VA health care facility is planning for new or revised clinical areas, the Facility Privacy Officer must be involved in the initial discussions so that the reasonable privacy safeguards are met.*

(4) Use of fax or email to disclose personally identifiable information must be appropriately secured and strictly adhere to this directive.

(5) VHA employees must not maintain personal copies of VHA records nor access their own records using any VA electronic health record (EHR) system even when the system permits access.

(6) VHA employees may maintain required electronic logbooks with appropriate safeguards in place. No paper logbooks may be kept unless there is a mandatory regulation that requires the physical logbook.

(7) All VHA employees who need to remove or transport paper or electronic personally identifiable information or PHI in the performance of their official job duties must have prior written approval from their respective VA supervisor before removal of personally identifiable information or PHI from VA health care facilities.

5. INDIVIDUAL RIGHTS

a. **The Individual.**

(1) Individuals have the right to receive a copy of the VHA Notice of Privacy Practices concerning individually identifiable health information.

(2) Individuals have the right to access, view and obtain a copy of their own personally identifiable information, including PHI, contained in a VA System of Records or retrievable by the individual's name.

(3) Individuals have the right to request that VHA amend their personally identifiable information, including PHI, when the information is inaccurate, untimely, irrelevant or incomplete. This right to amendment must be granted unless authority to deny the request is present (see paragraph 8.a.(10)).

(4) Individuals have the right to an accounting of disclosures of their personally identifiable information.

(5) Individuals have the right to request that VHA send communications regarding individually identifiable health information by alternative means or to alternative locations. VHA must accommodate such requests if they are reasonable.

(6) Individuals have the right to request that VHA restrict the uses or disclosures of the individual's individually identifiable health information to carry out treatment, payment or health care operations. Individuals also have the right to request VHA to restrict disclosures of the individual's individually identifiable health information to next-of-kin, family or significant others involved in the individual's care. VHA is not required to agree to such restriction requests. However, if a restriction is granted, VHA must adhere to the restriction to which it has agreed, unless information covered under the agreed to restriction is needed to provide emergency treatment to a patient. VHA will not agree to a restriction of a use or disclosure required by law.

(7) Individuals have the right to file a complaint regarding VHA's use or disclosure of their individually identifiable health information with VHA. Individuals also have the right to file a complaint with the Office of Inspector General (OIG) or the Secretary of HHS-OCR, in accordance with 45 C.F.R. § 160.306, when the individual believes VHA did not comply with the provisions of the HIPAA Privacy Rule. This right is in addition to any rights that the individual has under the Privacy Act.

(8) Individuals have the right to refuse to disclose their Social Security Number (SSN) to VHA. The individual must not be denied any right, benefit or privilege provided by law because of refusal to disclose their SSN to VHA (see 38 C.F.R. § 1.575(a)).

(9) Individuals may choose to be excluded from the inpatient facility directory. Individuals may request exclusion from the facility directory during each inpatient admission, in accordance with the Facility Directory Opt-Out in the Community Care Procedure Guide at: https://vaww.vrm.km.va.gov/system/templates/selfservice/va_kanew/help/agent/locale/en-US/portal/554400000001031/content/554400000050778/Section-E-Patient-Counseling?query=opt%20out. ***NOTE:*** *This is an internal VA website that is not available to the public. The facility directory does not apply to ERs unless the patient is going to be admitted to an inpatient setting. The Facility Directory Opt-Out does not apply to outpatient clinics. Opting out of the facility directory does not override other legal authority to disclose the patient's health information or location (e.g., request from or warrant from a law enforcement authority or to a family member when it is in the best interest of the patient).*

(10) If a competent individual is unable to physically sign a privacy-related form or request, such as an authorization or amendment request, due to a physical limitation or disability, the form will require two adult witnesses to authenticate the symbol or mark executed or adopted by the individual to indicate the individual's present intention to sign the form or request. If no symbol or mark can be made by the individual, the form must briefly document the circumstances of the signature and two adult witnesses to authenticate the individual's intent to sign the form or request.

b. **Personal Representatives of the Individual.** The personal representative of an individual has the ability to exercise the individual's rights stated in paragraph 5.a. A personal representative for the purposes of this directive does not necessarily equate to a surrogate for the informed consent process (see 38 C.F.R. § 17.32(e) for authorized surrogates for informed consent) or as a legally authorized representative for research. The following paragraphs provide details on various types of personal representatives for the purposes of this directive.

(1) **Power of Attorney.** A power of attorney (POA) is a written document in which an individual (i.e., principal) appoints another individual to act as the first individual's agent and gives authority to the agent to perform certain specified acts or kinds of acts on behalf of the principal. Each individual POA must be read for specificity of the intended purpose prior to any disclosure of any personally identifiable information. A POA that does not include decisions related to health care in its scope would not authorize the holder to exercise the individual's privacy rights.

(a) Types of POA include:

1. General Power of Attorney. General power of attorney (GPOA) provides broad authority for the agent to act on behalf of the principal. GPOA is often written in very general terms, giving the agent the power to act in a variety of situations, including the releasing or obtaining of information on behalf of the principal. GPOA must explicitly address health-care-related matters to authorize the agent to act on behalf of the principal for health care privacy rights.

2. Special or Limited Power of Attorney. A special or limited POA gives limited authority to an agent for a particular purpose or to perform a particular function (e.g., cash a check). Two examples of a special or limited POA are VA Form 21-22, Appointment of Veterans Service Organization as Claimant's Representative, and VA Form 21-22a, Appointment of Individual as Claimant's Representative. These two special or limited POAs enable a third-party to act on behalf of a Veteran claimant seeking benefits (including health care benefits) from VA (see 38 C.F.R. § 14.631).

3. Durable Power of Attorney for Health Care (i.e., Advance Directive). Pursuant to State law and VA policy, a patient may appoint a specific health care agent to make medical decisions on behalf of the patient if the patient becomes incapable of doing so. This includes decisions such as whether to release or obtain health records and other information about the patient, or how such information can be used. VA Form 10-0137, VA Advance Directive: Durable Power of Attorney for Health Care and Living Will, may be used to make such an appointment. Information about use of VA Form 10-0137 is found in VA Form 10-0137a, What You Should Know About Advance Directives. A durable POA expires upon death of the individual. ***NOTE:*** *For further information on Durable Power of Attorney for Health Care, see VHA Handbook 1004.02, Advance Care Planning and Management of Advance Directives, dated December 24, 2013.*

(b) Regardless of the type of POA that is presented, the reviewer must always carefully check the document to ensure that it meets the following requirements.

1. General and special POA must be:

a. In writing.

b. Signed by the principal (i.e., individual giving the power).

c. Dated.

d. Notarized and signed by a licensed notary public, except that VA Forms 21-22 or 21-22a and Advance Directives need not be notarized.

e. General and specific POA must specifically designate, by name, a third-party agent, which may be an individual, organization or other entity, to act on behalf of the principal.

2. The document must indicate the specific acts that the principal has authorized the agent to perform, such as reviewing or releasing health records.

3. The original signed POA is preferred; however, a photocopy of the POA may be accepted.

4. If there is some question regarding the competency of the principal to make decisions, the reviewer needs to determine if the POA authorizes the agent to act even if the principal is deemed to be medically or legally incompetent. A Durable Power of Attorney for Health Care necessarily operates only if the principal is incapable of making decisions. Otherwise, if there is no language to that effect in the POA, then the POA is inoperative so long as the principal is determined to be incompetent. In such cases, contact the local Office of Chief Counsel in the District for guidance.

5. Even if an original POA is presented, VHA employees are not required to honor the POA if there is some question regarding the authenticity of the document, or if there are other legal or administrative bases for questioning whether the person holding the POA is acting in the best interest of the principal. In such cases, contact the local Office of Chief Counsel in the District for guidance.

(2) **Legal Guardian.** Depending on the circumstances involved, a court may appoint a legal guardian for a specific purpose. A legal guardian is a person appointed by a court of appropriate jurisdiction to make decisions for an individual who has been judicially determined to be incompetent. A close reading of the court appointment is required to determine the authority of the legal guardian. Three of the most common types of guardianships are as follows:

(a) Legal Guardian of the Person. A legal guardian of the person is an individual appointed by a court of competent jurisdiction to make decisions regarding the personal welfare of an individual. This includes making decisions regarding the incapacitated individual’s health, requesting health records and authorizing the release of such records to third parties.

(b) Legal Guardian of the Property. A legal guardian of the property is an individual appointed by a court of competent jurisdiction to make decisions on behalf of another regarding property-related matters. This includes handling funds, real property and financial transactions on behalf of an individual. Generally, a legal guardian of the property does not have the authority to obtain access to or release health records unless the guardian can establish that the purpose for the release is related to property-related matters affecting the incapacitated individual.

(c) Legal Guardian of the Person and Property. Often a court of competent jurisdiction will appoint an individual as both legal guardian of the property and the person. In such cases, the legal guardian has the authority to make all decisions regarding the person and the property of that person, including obtaining access to and authorizing the release of, the person's health records.

(3) **Other Authority to Act on Behalf of a Living Individual.**

(a) Federal Law. If a Federal law authorizes a person to act on behalf of a living individual, that person is considered a personal representative for the purposes of this directive. VHA may disclose personally identifiable information pursuant to a written authorization from a personal representative.

(b) Other Law. If, under applicable State, local or tribal law, a person has authority to act on behalf of a living individual (e.g., the parent of unemancipated minor), that person is considered a personal representative for the purposes of this directive. VHA may disclose personally identifiable information pursuant to a written authorization from such personal representative.

(4) **Authority to Act on Behalf of a Deceased Individual.**

(a) Legal Authority. If a Federal, State, local or tribal law authorizes a person to act on behalf of a deceased individual or the deceased individual's estate (e.g., as executor), that person is considered a personal representative of the deceased for the purposes of this directive along with the surviving next-of-kin as outlined below. ***NOTE:*** *For disclosures of personally identifiable information on a deceased individual see paragraph 33.*

(b) Next-of-Kin. The next-of-kin of a deceased individual will be considered a personal representative of the deceased for the purposes of this directive. When there is more than one surviving next-of-kin, the personal representative will be determined based on the following hierarchy: spouse, adult child, parent, adult sibling, grandparent, adult grandchild or close friend. All individuals in the same level in the hierarchy will be equally treated as the personal representative of the deceased individual. Any dispute or conflicts in the next-of-kin hierarchy must be referred to the local Office of Chief Counsel in the District. ***NOTE:*** *The next-of-kin is not a personal representative of a living individual, unless authorized by one of the provisions noted above.*

6. NOTICE OF PRIVACY PRACTICES (IB 10-163)

a. VHA as a health plan is required, by the provisions of the HIPAA Privacy Rule, to provide all individuals who are beneficiaries of VHA health benefits (e.g., Veterans, caregivers and the Civilian Health and Medical Program (CHAMPVA)) with a notice of VHA's privacy practices. IB 10-163, VHA Notice of Privacy Practices, is provided to beneficiaries of VHA health benefits upon enrollment and every 3 years thereafter as outlined in VHA Handbook 1605.04. An individual has the right to request a copy of the VHA Notice of Privacy Practice at any time. The VHA Notice of Privacy Practices details the uses and disclosures of the individual's individually identifiable health information that may be made by VHA, as well as the individual's rights, and VHA's legal duties with respect to individually identifiable health information.

b. VHA as a health care provider must provide a copy of the VHA Notice of Privacy Practices to all non-Veteran patients who are not beneficiaries of VHA health benefits (e.g., humanitarian, employees, Fourth Mission, Service members and non-VA Veteran research subjects participating in VA studies involving clinical interventions) receiving care or treatment at a VA health care facility at the episode of care when the non-Veteran patient checks in for an appointment or when the non-Veteran patient is admitted to the hospital. VHA must seek an acknowledgement of the VHA Notice of Privacy Practices from all non-Veteran patients as outlined in VHA Handbook 1605.04.

c. An individual has the right to request an electronic or paper copy of the VHA Notice of Privacy Practices.

d. An individual who has questions regarding the VHA Notice of Privacy Practices should be referred to the Facility Privacy Officer.

e. The VHA Notice of Privacy Practices is not available in any official foreign language translations.

7. INDIVIDUALS' RIGHT OF ACCESS

a. **Verification of Identity.**

(1) Individuals who request information from their VHA records must provide sufficient information to verify their identity and to provide assurance that they are not improperly given access to records pertaining to someone else. Currently, VHA policy does not allow an individual to verify identity by email except through Secure Messaging.

(2) When an individual appears in person, verification of identity is typically through various forms of identification that an individual is likely to have available, such as a Veteran Health Identification Card (VHIC), passport, driver's license or employee identification card or comparison with image in the EHR. While current forms of identification are preferred, expired forms of identification are acceptable for this purpose. If the individual's identity cannot be verified in person, the request for information will be denied.

(3) For requests for information via mail, fax or digital image, the individual's signature must be used to verify identity along with the identification information provided with the request. Requests for information via mail, fax or digital image where suitable identification information, such as full name or date of birth, is not provided to permit VHA to adequately locate the information requested, even after it has been requested by VHA, will be denied under FOIA due to failure to adequately describe records sought.

b. **Right of Access or Review of Records.**

(1) Requests from individuals for access to review their individually identifiable information in its original form or obtain copies of their individually identifiable information must be processed in accordance with all Federal laws, including 38 U.S.C. §§ 5701 and 7332, FOIA, the Privacy Act and the HIPAA Privacy Rule. Except as otherwise provided by law or regulation, individuals, upon signed written request, are entitled to gain access to, or obtain copies of, their individually identifiable information or any other information pertaining to them that is maintained in any System of Records or designated record set maintained by VHA. This is a privacy right of access. Individuals do not have to state a reason or provide justification for wanting to see or to obtain a copy of their requested information. ***NOTE:*** *VA Form 10-5345a, Individuals' Request for a Copy of Their Own Health Information, may be used, but is not required, to fulfill the signed written request requirement.*

(2) All written requests to review, or obtain copies of, records must be received by mail, fax, in person or by mail referral from another agency or VA office. All right of access requests must be delivered to and reviewed by the System Manager for the VHA System of Records (i.e., person responsible for the records) in which the records are maintained, the Facility Privacy Officer or the designee of either of those positions. For further information, see VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, dated August 19, 2013.

(3) In determining whether to grant a right of access request, the responsible VHA employee must consider whether:

(a) The identity of the requester can be verified.

(b) The request for information complies with the right of access procedures outlined in paragraph 7 of this directive.

(c) The information is in the individual's record retrieved by the individual's name or unique identifier or is information pertaining to the individual in the system when a dually retrieved record.

(d) The information requested has been compiled in reasonable anticipation of a civil action or proceeding.

(e) The System of Records under which the information is covered is exempt from the right of access in accordance with applicable laws, including the Privacy Act and the HIPAA Privacy Rule (e.g., 103VA07B, Police and Security Records-VA).

(f) The information has been created or obtained in the course of research that includes treatment and the right of access has been temporarily suspended for as long as the research is in progress, provided that the individual agreed to the denial of access when the individual consented to participate in the research.

(4) When granting a right of access request, the System Manager for the concerned VHA System of Records, the Facility Privacy Officer or designee must take reasonable steps to limit the disclosure to information pertaining only to the individual making the request. If the information to be provided in response to an individual's request includes information regarding another individual, the information regarding the other individual is provided only if the information also pertains to the requester. ***NOTE:*** *Even though the Sensitive Patient Access Report (SPAR) in VistA and Access Audit Log in P2Sentinel for sites using the Oracle Cerner EHR contain employee names, a Veteran still has a first-party right of access to these reports because they are covered under the Privacy Act System of Records 79VA10A7, Veterans Health Information Systems and Technology Architecture (VistA)-VA.*

(5) Right of access requests for access to view a record must be processed as follows:

(a) When individuals appear in person at a VA health care facility, they must be advised at that time whether right of access or review of records can be granted at that time. When immediate review cannot be granted because the records must be retrieved from an off-site storage location such as National Archives and Records Administration (NARA) Records Center, commercial records storage or because the record must be made comprehensible to an individual (e.g., reproducing magnetic tape records in a hard copy form readable by the individual), necessary arrangements must be made for a later personal review or, if acceptable to the individual, copies may be furnished by mail.

(b) Requests for right of access received by mail must be referred by the System Manager for the VHA System of Records in which the records are maintained, the Facility Privacy Officer, or the designee of either position, who will determine whether the right of access request will be granted. If additional information is required before a request can be processed, the individual must be advised what information must be provided to complete the request. When a request for review of records will be granted, the individual must be advised by mail that access to view will be given at a designated location, date and time in the facility or a copy of the requested record will be provided by mail, if the individual has indicated that a copy is acceptable.

(6) Right of access requests for copies of a record must be processed as follows:

(a) Requests received by fax are acceptable only after confirmation has been obtained from the individual to whom the record pertains or through other verification process, such as review of the signature on the request. The request must be referred to the System Manager for the VHA System of Records in which the records are maintained, the Facility Privacy Officer, or the designee of either position, who determines whether access will be granted. The request will be processed and copies provided by fax for an emergent response; otherwise, the request is processed the same as a request received by mail.

(b) When a request for records is transferred or referred from another Federal agency or VA office to a VA health care facility, the VA health care facility processes the request in the same manner as a request received via mail.

(c) Email requests from Veterans or patients will not be accepted, except through Secure Messaging as discussed below, until such time as VHA can authenticate the identity of the email sender and accept an electronic signature within an email. Email requests from VHA employees for copies of their Employee Medical File will be accepted when signed using the employee's PIV card.

(d) A scanned or digital image of a signed, written request, such as a portable document format (PDF), received via email will be accepted only after confirmation has been obtained either from the individual to whom the record pertains or through other verification process, such as review of the signature on the request. If additional information is required in order to process the request, any communication with the individual via email must follow VA Directive 6500, VA Cybersecurity Program, dated February 24, 2021, and VA Handbook 6500.

(e) The Electronic Signatures in Global and National Commerce Act, Public Law 106-229 addresses the requirements for a legally effective electronic signature. VA must comply with OMB M-21-04 and accept remote identity-proofing and authentication for the purpose of allowing individuals to request copies of their VHA records covered by the Privacy Act electronically.

1. Electronic requests received through VA information technology (IT) software and applications, such as VA Blue Button and Mobile Applications, will be accepted and processed automatically within the software or application requiring no action by the System Manager for the VHA System of Records in which the records are maintained, the Facility Privacy Officer or the designee of either position.

2. Electronic requests received through Secure Messaging will be accepted as long as the Veteran's typed name, which fulfills the signature requirement, is present. Verification of identity occurs within the system where Secure Messaging is accessed through logon and authentication processes. For more information, see the Health Information Management (HIM) Release of Information (ROI) Program Guide, available at: https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/roi.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

(7) Whenever a request for review in person of individually identifiable information is approved, the following procedures apply:

(a) A VHA employee must always be present during any personal review of a record, even if the records to be reviewed are paper records. If the review is of electronic records, the System Manager for the concerned VHA System of Records, Facility Privacy Officer or the designee of either position must appoint a VHA employee to navigate through an electronic record to ensure the integrity of the record. An individual who is not an employee cannot be given direct access, use an employee's access or be left unattended when viewing the individual's own electronic record.

(b) Pursuant to 38 C.F.R. § 1.577(a) and VA Handbook 6300.4, a person of the individual's own choosing may accompany the individual to review a record. The individual must provide signed, written authorization such as VA Form 10-5345, Request for and Authorization to Release Health Information.

(8) **Time Frames.**

(a) VA health care facilities must process all requests for review or copies of individually identifiable information within 20 business days (excluding weekends and Federal holidays) of receipt of the request, whenever possible. If the right of access request cannot be processed within the 20-business-day period, an acknowledgment letter of the request must be sent to the requester within the same 20 business days.

(b) When, for good cause, a facility is unable to provide the requested information in a record within the 20-business-day period, the individual must be informed in writing of the reasons why access cannot be provided within the required time frame. The facility must also state when it is anticipated that the record will be available, and this must not exceed 40 business days from receipt of request.

(9) **Fees.** An individual requesting a copy of records or information under right of access must be provided the first copy of the requested record or information free of charge. After the first copy, fees are charged in accordance with 38 C.F.R. § 1.577.

c. **Denial of Access.**

(1) A valid right of access request for a record may be denied only in very limited circumstances, and the Facility Privacy Officer must be consulted prior to such denial. For example, an otherwise valid request for access to a record may be denied based on a relevant Privacy Act exemption.

(2) When a right of access request to a record is denied, the System Manager for the VHA System of Records in which the record is maintained, the Facility Privacy Officer or the designee of either position must promptly prepare a notification to the individual of the decision. This notification must:

(a) State the reason for the denial.

(b) Inform the individual of their right to appeal in writing to OGC (024), at Department of Veterans Affairs, 810 Vermont Avenue N.W., Washington, DC 20420.

(c) Be signed by the VA medical facility Director or designee for records maintained by a VA medical facility or Facility Privacy Officer for other records.

8. RIGHT TO REQUEST AMENDMENT OF RECORDS

a. **General.** An individual has the right to request an amendment to any information or records retrieved by the individual's name or other individually identifiable information contained in a VA System of Records, as provided in 38 C.F.R. § 1.579 and 45 C.F.R. § 164.526. The right to seek an amendment of this information or records is a personal right of the individual to whom the record pertains. The personal representative of a deceased individual has a right to request an amendment of the decedent's records.

(1) An amendment request must be in writing, signed and must adequately describe the specific information the individual believes to be inaccurate (i.e., faulty or not conforming exactly to truth), incomplete (i.e., unfinished or lacking information needed), irrelevant (i.e., inappropriate or not pertaining to the purpose for which records were collected) or untimely (i.e., before the proper time or prematurely) and the reason for this belief.

(a) A scanned, digital image or fax of a written, signed request will be accepted.

(b) An amendment request submitted by Secure Messaging through a Patient Portal, such as MyHealth*e*Vet, to the facility Privacy Officer explicitly that contains the required information and where the identity of the individual submitting the request can be authenticated will be accepted.

(2) If a competent individual is unable to physically sign a form due to a physical limitation or disability, the form must be witnessed as required by paragraph 5.a.(10).

(3) The written amendment request must be routed to the Facility Privacy Officer for the VHA System of Records in which the records are maintained or for a VA medical facility to the VA medical facility Privacy Officer or Chief, HIM as determined by local procedures. Amendment requests are to be maintained by the Facility Privacy Officer in accordance with VHA RCS 10-1 and must not be filed within the Veteran's record unless, after denial of the amendment request, a statement of disagreement has been received from the Veteran or the Veteran has requested their amendment request letter and the facility's subsequent denial letter be affixed to the disputed record.

(4) The individual may be asked to clarify a request that lacks specificity in describing the information for which an amendment is requested so that a responsive decision may be reached.

(5) A request for name change is considered an amendment request and must be referred to the Master Patient Index (MPI) Coordinator for processing. Appropriate legal documents for the MPI Coordinator to make the name change are required and outlined

in VHA Directive 1906, Data Quality Requirements for Health Care Identity Management and Master Veteran Index Functions, dated April 10, 2020. For additional instruction, see the Practice Brief, Processing Amendment of Records in Electronic Health Record Systems under Privacy Laws, dated September 2022, available at: https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/FactSheets.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

(6) The VHA employee who authored or is responsible for the information that is the subject of the amendment request must review and determine whether to approve or deny the amendment request. This review must be guided by the criteria set forth in 38 C.F.R. § 1.579. That is, VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant and necessary to accomplish a purpose of VA, as required by law, regulation, Executive Order of the President, or a Government-wide or VA policy implementing such a purpose. These criteria must be applied whether the request is to modify a record, to add information to a record or to delete information from a record.

(7) When an individual requests amendment of clinical or health information in the EHR of a VA medical facility, the VA medical facility Privacy Officer or Chief of HIM as determined by local procedures, must refer the request and related record to the VA health care provider or clinical staff member who is the author of the information to determine if the record needs to be amended.

(a) If the VA health care provider or clinical staff member is no longer at the VA medical facility, a health care provider or clinical staff member designated by the VA medical facility Director must determine if the record needs to be amended.

(b) VA health care providers and clinical staff are not allowed to amend, modify, revise or edit another provider's signed or authenticated clinical documentation or note unless they are the Supervising Practitioners over a Health Professions Trainee (HPT). The placement of an addendum is not considered an amendment, modification, revision or edit for these purposes. VA health care providers and clinical staff may not process a privacy amendment request to amend or modify their own signed or authenticated clinical documentation or notes from a patient. All such requests must be referred to the VA medical facility Privacy Officer. VA health care providers and clinical staff may make administrative corrections as outlined in VHA Directive 1907.01, VHA Health Information Management and Health Records, dated April 5, 2021. ***NOTE:*** *An administrative correction is remedial action by appropriate personnel with the authority to correct information previously captured by, or in, error regardless of who makes VHA aware of the error. Examples of items that can be handled as an administrative correction are incorrect date, association or linking data to wrong patient, or other designated clinical data items impacting the integrity of the record.*

(8) **Timeframes.** A request to amend a record must be acknowledged in writing within 10 business days of receipt unless the amendment is processed fully within those 10 business days. If a determination whether to honor the request has not been made within this time period, the Facility Privacy Officer or designee must advise the individual

when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 business days from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay shall not exceed 90 calendar days from receipt of the request.

(9) **Approval of Privacy Amendment Request.** When a request to amend a record is approved by the author or designee, the Facility Privacy Officer or designee must take the following actions:

(a) Any information to be deleted that is maintained in non-electronic form must be made illegible (e.g., marked through in the paper record). Any new material must be recorded on the original document. The words "Amended-Privacy Act, Amendment Filed, or 45 C.F.R. Part 164" must be recorded on the original paper document. The new amending material may be recorded as an addendum if there is insufficient space on the original document. The original document must clearly reflect that there is an addendum and care must be taken to ensure that a copy of the addendum accompanies the copy of the original document whenever it is used or disclosed. The amendment must be authenticated with the date, signature and title of the person making the amendment.

(b) For an electronic privacy amendment of the health information in the EHR, the request must be referred to the VA medical facility Privacy Officer or Chief of HIM as determined by local procedures, for action within the EHR. ***NOTE:*** *For a TIU (Text Integration Utility) document within VistA/Computerized Patient Record System (CPRS), the Chief of HIM or designee is responsible for utilizing the TIU AMEND action for all TIU documents. If the original document cannot be amended and an addendum cannot be attached, then a link to the location of the amendment must be provided. For an electronic privacy amendment to health information within Oracle Cerner EHR, the Chief of HIM or designee is responsible for utilizing the Modify-Revise or In Error functionality within the appropriate Oracle Cerner EHR application.*

(c) The individual making the request for amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The written response provided by the Facility Privacy Officer or designee must also notify the individual that the entities who have previously received the amended information must be identified for the amended health information to be shared with these entities.

(d) The Facility Privacy Officer or designee must notify all relevant persons or organizations to which the facility disclosed the amended information. If 38 U.S.C. § 7332-protected health information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations unless authority exists to permit sharing.

(e) If the record has been disclosed prior to amendment to a Business Associate, the Business Associate must be informed of the correction and provided with a copy of the

amended record. ***NOTE:*** *The accounting of disclosures summary may be utilized to determine recipients of the information subject to the amendment.*

(10) **Denial of Amendment Request.** When a request to amend a record is denied, the Facility Privacy Officer or designee must promptly notify the individual making the request of the facility decision.

(a) The written notification must:

1. State the reasons for the denial. VHA may deny a request to amend a record if VHA finds that the individually identifiable information or record requested to be amended:

a. Was not created by VHA and the originator of the individually identifiable information is another Federal agency available to act on the request. In this instance, the individual will be informed that the individual needs to request that the originating Federal agency of the individually identifiable information amend the record. If, however, the originating Federal agency of the individually identifiable information is no longer available to act on the request or authorizes VA to decide whether to amend the record, then VHA must do so.

b. Is accurate, relevant, complete or timely in its current form.

c. Is not part of a VHA System of Records or designated record set.

2. Advise the individual that the denial may be appealed to OGC and include the procedures for such an appeal as noted below in paragraph 8.b.

3. Advise the individual that if an appeal is not filed and a statement of disagreement is submitted, the statement of disagreement cannot exceed three pages and may still be submitted to the facility for linking to the disputed record.

4. Advise the individual that if an appeal is not filed or a statement of disagreement is not submitted, the individual may still request that the VA health care facility provide the individual's request for amendment and the denial with all future disclosures of the information. This request must be submitted in writing to the Facility Privacy Officer or designee.

5. Describe how the individual may file a complaint with VHA or the Secretary, HHS. The description must include the name or title and telephone number of the contact person or office.

6. Be signed by the Facility Director or designee.

(b) If requested by the individual, the Facility Privacy Officer or designee must identify the individually identifiable information that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment and the facility's denial of the request to the individual's record.

(c) If the amendment does not pertain to the Veteran's health record, the Facility Privacy Officer will work with the appropriate System Manager for the VHA System of Records in which the information is maintained following the same amendment process as above.

b. **Appeal of Initial Adverse Department Determination of Amendment.**

(1) An individual may appeal a denial, in whole or in part, of a request for correction or amendment of individually identifiable information in VHA Privacy Act Systems of Records or designated records sets to OGC.

(a) The written appeal must be mailed or delivered to OGC (024), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420.

(b) The letter of appeal must clearly indicate why the individual disagrees with the initial denial, with specific attention to one or more of the four standards (i.e., accuracy, relevance, timeliness and completeness) and include a copy of the facility denial letter as well as any supporting documentation that demonstrates why the individual believes that the clinical information does not meet these requirements.

(2) When OGC finds, on appeal, that the adverse determination must be reversed, in whole or in part, the individual and the VA health care facility must be notified of the decision. Upon receipt of the notification, the System Manager for the VHA System of Records in which the information is maintained, the Chief of HIM, the Facility Privacy Officer or the designee for any of those positions, must amend the record as instructed in the notification. ***NOTE:*** *The amendment procedures established above in paragraph 8 must be followed.*

(3) If General Counsel or Deputy General Counsel sustains the adverse decision, the appeal decision letter must advise the individual of the right to file a concise written statement of disagreement with the VA health care facility that made the initial decision.

(4) A statement of disagreement can be submitted by an individual prior to appealing to OGC. For more information on statement of disagreements see paragraph 8.c. below.

c. **Statement of Disagreement.**

(1) A statement of disagreement is a concise written statement setting forth the reasons for or basis of disagreeing with the denial of all or part of a requested amendment. A statement of disagreement may be filed by the individual whose amendment request was denied either within 30 calendar days after receipt of a final decision from OGC on appeal or within 365 calendar days of the original denial if an appeal to OGC is not filed.

(2) The HIPAA Privacy Rule permits VHA to reasonably limit the length of a statement of disagreement. VHA has determined that three pages is a reasonable length to permit a concise statement of disagreement. Any statement of disagreement

received that is longer than three pages will be returned to the individual with reference to this directive and a request to submit a statement of disagreement that is three pages or less.

(3) When an individual files a statement of disagreement, the record about which the statement pertains must be clearly annotated to note which part of the record is disputed. The individual's statement of disagreement, any rebuttal prepared by the facility, the individual's request for an amendment and the facility's denial of the request in this order must be appended or otherwise linked to the individual's record. When the statement of disagreement is filed separately from and only linked to the disputed record, an addendum or note must be added to the disputed record to notate the location of the linked documents.

(4) Once a statement of disagreement is filed, a review of previous disclosures of the disputed records needs to be conducted to determine the persons or organization that has received the disputed information. The System Manager for the concerned VHA System of Records, or designee, or the Facility Privacy Officer, or designee, must obtain the individual's agreement to notify the relevant persons or organizations with which the statement of disagreement needs to be shared. If 38 U.S.C. § 7332-protected information is disputed, the individual must provide written authorization to allow the sharing of the statement of disagreement with persons or organizations that previously received the disputed information.

(5) When future disclosures are made of the disputed record, a copy of the statement of disagreement must be provided. A copy of a concise statement of VA's reasons for not making the amendments requested or rebuttal, when prepared, must also be provided.

(6) A VA health care facility may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the System Manager for the concerned VHA System of Records or designee, or the Facility Privacy Officer, or designee, must provide a copy to the individual who submitted the statement of disagreement. In addition, the rebuttal must also be linked to the disputed record.

d. **Documents for Facility Privacy Amendment File.**

(1) The Facility Privacy Officer must keep all privacy amendment requests for records maintained by their respective VA health care facilities in an organized file by date. This file must contain all of the following documents:

(a) The original initial amendment request.

(b) VHA responses to the amendment request (e.g., interim or final response letter and letters to previous recipients of the health record).

(c) Clarifying letters to requester or documentation of telephone discussions (i.e., reports of contact).

(d) Acknowledgement letter to requester if response cannot be provided within 10 business days.

(e) Any other correspondence received from or with the individual requester, including the statement of disagreement, if provided.

(f) Email or other correspondence (e.g., memos) addressed to providers or authors of the disputed record initiating review of amendment request.

(g) All provider or record author responses regarding decision to amend or deny amendment.

(h) Copy of the portion of the health record that is the subject to amendment request, and a copy of the amended health record, if the amendment has been granted.

(i) Any written facility rebuttal to individual's statement of disagreement, if applicable.

(j) Any correspondence from OGC regarding the amendment request.

(k) Accounting of disclosure records. ***NOTE:*** *If there is no accounting of disclosures for the health records in question, the Facility Privacy Officer can include a screen shot from the Release of Information (ROI) Plus to document that this has been verified. Amendment requests are not tracked in the ROI Plus software, because they are not considered disclosures. See VHA Directive 1615, Mandated Utilization of Release of Information (ROI) Plus Software, dated March 23, 2022, for further information.*

(2) The amended record must be maintained for the life of the agency record. For example, an amended progress note must be maintained for the life of the patient medical record.

(3) The amendment file must be retained and destroyed in accordance with RCS 10-1, section 1006.9, Privacy Act Amendment Request Files. The amendment files are not scanned into the Veteran's health record as they are not considered part of the health record. They must be maintained in a secure manner such as a locked file cabinet or scanned to a secure network drive but cannot be scanned into the EHR.

9. ACCOUNTING OF DISCLOSURES FROM RECORDS

a. An individual may request a list of disclosures of information from records pertaining to them, subject to the provisions of 38 C.F.R. § 1.576(c) and 45 C.F.R. § 164.528.

b. The request for an accounting of disclosures must be in writing, signed and must adequately identify the VHA System of Records or designated record sets for which the accounting is requested. The written request must be mailed, or delivered, to the VA health care facility that maintains the record and directed to the attention of the Facility Privacy Officer or designee or the System Manager for the VHA System of Records from which the accounting is being requested.

c. The individual must be provided with an accounting that includes:

(1) The name of the individual to whom the information pertains.

(2) The date of each disclosure.

(3) Nature or description of the information disclosed.

(4) A brief statement of the purpose of each disclosure or, in lieu of such statement, a copy of a written request for a disclosure.

(5) The name and, if known, address of the person or agency to whom the disclosure was made.

d. The accounting of disclosures must be made available upon request to the individual to whom the record pertains within 60 calendar days after receipt of such a request; except disclosures made for law enforcement purposes, which will not be made available except as provided by 38 C.F.R. § 1.576(b)(7) and 45 C.F.R. § 164.528(a)(2)(i). If the accounting cannot be provided within the specified timeframe, the facility or program can extend the timeframe for no more than 30 calendar days, provided that the individual is given a written statement of the reasons for the delay and the date by which the accounting will be provided. ***NOTE:*** *Only one such extension of time for action on a request for an accounting is allowed.*

e. The accounting or disclosure summary given to an individual must be provided without charge.

f. VHA must retain a copy of the disclosure summary provided to the individual for six years after the date of disclosure or the life of the record whichever is longer (see RCS 10-1 or the Facility Records Control Officer).

10. CONFIDENTIAL COMMUNICATIONS

a. An individual has the right to request and receive communications (e.g., correspondence) confidentially from VHA by an alternative means or at an alternative location. VHA considers an alternative means to be in person (rather than by mail) and considers an alternative location to be a mailing address other than the individual's permanent or home address listed in the VA Profile and MPI or EHR. ***NOTE:*** *An individual's preference to communicate with VA through communication mechanisms such as email, voicemail and text messages is not the exercise of the right to receive communications from VHA confidentially.*

b. Before providing the information by an alternative means or at an alternative location, the responsible facility official must verify the individual's identity in accordance with the procedures contained in paragraph 7 of this directive.

c. VHA must accommodate reasonable requests from the individual to receive communications either at an alternative address or in person at the VA health care facility where the information is maintained.

d. If a Veteran requests to use their cell phone number as an alternate means of verbal communication, they should be directed to Enrollment and Eligibility Office within the VA medical facility. Currently, no electronic process to alert staff to use this number as an alternative "confidential" verbal communication is available. ***NOTE:*** *A request to receive confidential communications from VHA via personal email is considered unreasonable and therefore will be denied. Secure Messaging may be used for this purpose.*

e. When documenting confidential communications in VistA, all communications or correspondence fit into one of five following correspondence types:

(1) Eligibility or enrollment.

(2) Appointment or scheduling.

(3) Co-payments or Veteran billing.

(4) Health records.

(5) All other.

f. Requests to have all communications or just communications of a specific correspondence type, sent to the "confidential communications" address may only be accommodated at VA medical facilities still using VistA/CPRS. However, communications within each correspondence type will not be split (i.e., all communications within a single correspondence type must be directed to the same address). Requests to split communications under a correspondence type must be considered unreasonable and therefore must be denied. For additional guidance please see the Confidential Communication Guidance at: https://vaww.vrm.km.va.gov/system/templates/selfservice/va_kanew/help/agent/locale/en-US/portal/554400000001046/content/554400000106995/VAMC-Enroll-Elig-Address-Entry?query=address#Confidential. ***NOTE:*** *This is an internal VA website that is not available to the public.*

g. When a "confidential communications" address for health records has been entered in ROI Plus, the ROI Department must use this address to provide an individual with copies of their own health records regardless of the address on the written request unless the individual is contacted to address the discrepancy. The individual must also be informed to contact the Enrollment and Eligibility Office within the VA medical facility to update the address information in VistA.

11. RIGHT TO REQUEST RESTRICTION

a. An individual has the right to request VHA restrict its use or disclosure of individually identifiable health information for the purpose of treatment, payment or health care operations. An individual also has the right to request that VHA restrict the disclosures of the individual's individually identifiable health information to next-of-kin, family or significant others involved in the individual's care. VA health care providers and clinical staff are prohibited from granting any verbal restriction requests. Merely documenting a patient's request to restrict their information in their EHR does not constitute a restriction request.

b. Generally, VHA may not agree to grant a restriction request by a personal representative of a deceased Veteran or patient to restrict a family member's access to the deceased Veteran's or patient's PHI under FOIA.

c. VHA is not required to agree to any restrictions requested. ***NOTE:*** *45 C.F.R. § 164.522(a)(1)(vi) does not apply to VHA as it pertains solely to the disclosure of health information for a health care service or visit which the patient paid out-of-pocket in full and VHA is not legally permitted to accept out-of-pocket payments from a Veteran for the full cost of a VA health care service or visit.*

d. A restriction request must:

(1) Be in writing,

(2) Identify which information is to be restricted,

(3) Indicate for what purposes (e.g., use for payment) the identified information is to be restricted, and

(4) Be signed by the individual to whom the records pertain or their personal representative.

e. Before granting any request for restriction of individually identifiable health information, the Facility Privacy Officer must review the request and consult with the VHA Privacy Office by telephone or email on the decision. Denial of restriction requests do not need to be reviewed by the VHA Privacy Office.

f. If a request for restriction is granted, VHA must comply with the restriction unless the individual revokes the restriction in writing, the information covered by the agreed to restriction is needed to provide a patient with emergency treatment, or the restriction is terminated by VHA, as outlined in paragraph 11.j. The Facility Privacy Officer must add an alert regarding the restriction in the ROI Plus software and under the Crisis Warnings, Allergies and Directives (CWAD) in VistA/CPRS.

g. If a request for restriction is denied, VHA must notify the individual in writing of the denial.

h. There are no appeal rights when denying a restriction request.

i. General statements such as “No health information can be released to anyone but myself” or “I only want you to release information to my primary care providers” are not specific enough to constitute a restriction request that may be granted and must be denied. The individual needs to be directed to submit a more specific request.

j. VHA may terminate a granted restriction, if VHA informs the individual, in writing, that it is terminating its agreement to a restriction and that such termination is only effective with respect to PHI created or received after VHA has so informed the individual. Reasons for terminating a restriction include, but are not limited to, a status change in the individual’s competency, a major status change in the individual’s care or benefits and statutory revisions affecting the use or disclosure of the information restricted.

12. TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS

a. **Veterans Health Administration.**

(1) For purposes of this directive, personally identifiable information may be used on a need-to-know (Privacy Act) basis within VHA for purposes of treatment, payment or health care operations (HIPAA Privacy Rule), without the written authorization of the individual.

(2) Within VHA, use of information on a need-to-know basis for purposes other than treatment, payment or health care operations, such as research, requires a written authorization or other legal authority as described in this directive.

(3) The VHA Office of Research Oversight (ORO) enforces compliance with requirements for VA research in accordance with its responsibilities under 38 U.S.C. § 7307. ORO is not required to have a written authorization from subjects or provide a written request for PHI or other personally identifiable information when needed in connection with its compliance oversight responsibilities.

(4) The VHA Office of Medical Inspector (OMI) addresses health care problems to monitor and improve the quality of care provided by VHA. VHA OMI reviews for these purposes are covered under health care operations. However, when VHA OMI conducts reviews at the direction of the Secretary of Veterans Affairs to address an Office of Special Counsel (OSC) inquiry, the reviews are for health oversight.

b. **VA Entities.**

(1) **Personally Identifiable Information Excluding Health Information.** VHA may share personally identifiable information, excluding health information, to any component of VA that needs the information for the purposes of fulfilling VA’s mission or to any VA employee with a need for the information in the performance of their official duties without signed, written authorization. See 5 U.S.C. § 552a(b)(1).

(2) **Individually Identifiable Health Information and Protected Health Information.**

(a) VHA may disclose individually identifiable health information to other VA components that determine eligibility for or entitlement to, or that provide benefits under the laws administered by the Secretary of Veterans Affairs without the signed, written authorization of the individual. The only VA components that determine eligibility for or entitlement to, or that provide benefits to Veterans are VHA, the Veterans Benefits Administration (VBA), the Board of Veterans Appeals (BVA) and the National Cemetery Administration (NCA).

(b) VHA may disclose individually identifiable health information with VA components for the purposes of VHA's own treatment, payment or health care operations. In this scenario, the VA component is not providing a covered function or acting on behalf of VHA.

(3) VHA may disclose individually identifiable health information with VA components who provide treatment, payment or health care operations or other covered functions on behalf of VHA without the signed, written authorization of the individual as long as a national BAA is in effect as outlined in VA Directive 6066, Protected Health Information and Business Associate Agreements Management, dated September 2, 2014. Before disclosing PHI, contact the VHA Privacy Office to confirm the existence of a BAA or check online at: http://vaww.vhadataportal.med.va.gov/DataAccess/BusinessAssociateAgreements.aspx . ***NOTE:*** *This is an internal VA website that is not available to the public.*

c. **Office of General Counsel.**

(1) VHA may provide all information, including personally identifiable information and 38 U.S.C. § 7332-protected information, to OGC for any official purpose authorized by law.

(2) VHA must maintain a national BAA with OGC for authorizing the sharing of PHI with OGC for legal counsel provided to VHA under health care operations.

d. **VA Office of Information and Technology.**

(1) VHA may provide all information, including personally identifiable information and 38 U.S.C. § 7332-protected information, to the VA Office of Information and Technology (OIT) for any official purpose authorized by law.

(2) The VHA Privacy Office must maintain a national BAA with the OIT for authorizing the sharing of individually identifiable health information with OIT for IT services, security services and incident response.

e. **VA Contractors.**

(1) VHA may disclose or release individually identifiable health information to VA contractors for the purpose of the contractor performing a service related to VA treatment, payment or health care operations (i.e., a "use," without the signed-written authorization of the individual) as long as the use is within the scope of the contract and there is a signed BAA on file.

(2) Disclosing individually identifiable health information by VHA to VA contractors for purposes other than treatment, payment or health care operations requires other authority and potentially a DUA.

(3) The Facility Privacy Officer must be contacted prior to the release of any Veteran personally identifiable information to a VA contractor to ensure appropriate authority is in place. An accounting of disclosures is not required for sharing personally identifiable information with VA contractors.

(4) For guidance on BAAs see VHA Directive 1605.05.

(5) A nursing home with which VHA has a contract may be provided personally identifiable information, including health information for the purpose of fulfilling the contract for providing health care to Veterans housed in its facilities.

f. **Readjustment Counseling Service Vet Centers.**

(1) Vet Centers are part of VHA under the Office of Readjustment Counseling Service (RCS). However, Vet Centers operate separately from VA medical facilities and are not organizationally aligned within the VISN and Office of Operations chain of command. Vet Centers report to one of five District Offices and to RCS.

(2) Each District Office has a Facility Privacy Officer assigned to those Vet Center within their individual District to report privacy issues. VISN or VA medical facility Privacy Officers are not responsible for the Vet Centers that are physically located on the VHA property nor the ones located near VA health care facilities.

(3) Vet Centers must comply with VHA national privacy policies, including this directive. However, RCS has issued more stringent policy that still complies with the requirements of this directive and is to be followed by Vet Centers. For additional information see VHA Directive 1500(3), Readjustment Counseling Service, dated January 26, 2021, or contact RCS.

g. **Non-VA Entities.** VHA may disclose information outside VA for any purpose including treatment, payment or health care operations, only if appropriate legal authority exists or written authorization is obtained.

13. RESEARCH

This paragraph provides guidance only with regards to the Federal privacy and confidentiality laws affecting human subjects' research endeavors. Each VA medical facility must establish a review process to ensure these privacy requirements are met. The review process may involve the VA medical facility's Privacy Officer being a non-voting member or consultant of the facility Institutional Review Board (IRB) or Research and Development (R&D) Committee or a member of another research committee or subcommittee responsible for ensuring that all privacy and security requirements are met. While the VA medical facility Privacy Officer is the approving official for the written HIPAA authorization, the VA medical facility Privacy Officer does not provide the approval of the informed consent for research purposes. This directive does not negate or supersede any research statutes, regulations or policies. Research investigators must still ensure that appropriate authority exists to use or disclose information derived from or pertaining to individuals. ***NOTE:*** *The VA medical facility Privacy Officer is not responsible for the privacy reviews and approvals of specified research activities if an IRB MOU or IRB Authorization Agreement specifically states that the privacy reviews and approvals will be conducted by another VA medical facility Privacy Officer (e.g., the VA Central IRB Privacy Officer). See the VHA 1200 policy series, specifically VHA Directive 1200.01(1), Research and Development Committee, dated January 24, 2019, and VHA Directive 1200.05(3), Requirements for the Protection of Human Subjects in Research, dated January 7, 2019, for additional requirements for conducting research within VA*.

a. **Release of Information to VA Investigators (Intramural).**

(1) All research within VHA must be conducted by a VA Investigator and VHA personnel. A VA Investigator must be a VHA employee which includes official without compensation (WOC) or VA-Intergovernmental Personnel Act (IPA) of 1970 employees. ***NOTE:*** *To determine if a researcher is a VA Investigator, contact the VA medical facility's Associate Chief of Staff for R&D or facility's research office.*

(2) **Reviews Preparatory to Research.** VA Investigators may use personally identifiable information to prepare a research protocol prior to submission of the protocol to the IRB or R&D Committee for approval. The VA Investigators must not arbitrarily review PHI based on their access to PHI as a VHA employee until the investigator makes a representation that the access to PHI is only to prepare a protocol, that no PHI will be removed from the covered entity (i.e., VHA) and the access to PHI is necessary for preparation of the research protocol as required by the HIPAA Privacy Rule. The VA investigator must document this representation in a designated file and present this written document when requesting access to the information custodian. Non-VA researchers may not obtain VHA information for preparatory research activities.

(a) To access and use PHI "preparatory to research," neither a written HIPAA authorization from the individual nor a waiver of the requirement to obtain a HIPAA authorization by an IRB or Privacy Board are required.

(b) During the preparatory to research activities the VA Investigator:

1. Must only record aggregate data. The aggregate data may only be used for background information to justify the research or to show that there are adequate numbers of potential subjects to allow the investigator to meet enrollment requirements for the research study.

2. Must not record any individually identifiable health information. Any individually identifiable health information placed into the Veterans Affairs Informatics and Computing Infrastructure (VINCI) workspace as preparatory to research activities is permitted when the VA Investigator only records aggregate data. After the aggregate data is recorded, the individually identifiable health information must be removed from the VINCI workspace prior to the initiation of the research study. When individually identifiable health information is not removed from the VINCI workspace following the VA Investigator's recording of the aggregate data prior to the initiation of the research study, the use of the individually identifiable health information is not a preparatory to research activity.

3. Must not use any personally identifiable information to recruit research subject.

(c) A DUA may be required by the data repository owner or custodian if personally identifiable information is transferred from a data repository to the VA investigator for their preparatory to research review. The DUA is to ensure the VA Investigator complies with the requirements of the above paragraph and returns or destroys the personally identifiable information once the review is completed. See VHA Handbook 1200.12.

(d) The contacting of potential research subjects or conducting pilot studies are not activities preparatory to research but activities to be undertaken and approved by the IRB, if required by VHA Directive 1200.05(3) and R&D Committee. Therefore, a written HIPAA authorization from the individual or a waiver of the requirement to obtain a HIPAA authorization by an IRB or Privacy Board are required for such activities.

(3) **VA-Approved Research.** All research activities involving human subjects or human data conducted by VA Investigators requires the responsible Facility Privacy Officer to review the research to ensure it complies with all applicable privacy requirements related to the information to be used and disclosed as outlined in VHA Directive 1200.01(1) and VHA Directive 1200.05(3). Research Privacy Reviews will be documented as required by VHA Directive 1605.03(2), Privacy Compliance and Accountability Program, dated September 19, 2019, using VA Form 10-250, VHA Research Protocol Privacy Review Checklist. ***NOTE:*** *The VA medical facility Privacy Officer is not responsible for the privacy reviews and approvals of specified research activities if an IRB MOU or IRB Authorization Agreement specifically states that the privacy reviews and approvals will be conducted by another Facility Privacy Officer (e.g., the VA Central Office IRB Privacy Officer).*

(4) All VA Investigators conducting VA-approved research must obtain appropriate legal authority to use personally identifiable information, including health information,

and to disclose personally identifiable information outside of VHA as part of the VA-approved research.

(5) VHA individually identifiable health information involving non-employee research subjects (e.g., Veterans, their beneficiaries, caregivers and patients) may be used by a VA investigator for research purposes provided there is a prior written HIPAA authorization that meets all requirements as identified in paragraph 14 of this directive as determined by the responsible VA medical facility Privacy Officer.

(6) A written HIPAA authorization may be incorporated into an informed consent for participation in research except when unconditioned/optional components are present, such as optional tissue banking, or the subjects have diminished decision-making capacity and informed consent will be obtained from the subject's legally authorized representative. ***NOTE:*** *Because VA subjects may revoke HIPAA authorizations, when the HIPAA authorization is combined with the informed consent, the document must clearly indicate whether revocation of the HIPAA authorization is also withdrawal of informed consent.*

(7) When not incorporated into the informed consent, VA Form 10-0493, Authorization for Use and Release of Individually Identifiable Health Information Collected for VHA Research must be used *for* the written authorization. ***NOTE:*** *The IRB does not approve HIPAA authorizations or whether the authorization may be combined into the informed consent. The responsible Facility Privacy Officer makes such determinations.*

(8) If there is no prior signed, written HIPAA authorization, VHA individually identifiable health information involving non-employee research subjects may be used by a VA Investigator for research purposes when there is an IRB or Privacy Board waiver of HIPAA authorization in accordance with 45 C.F.R. § 164.512(i). A waiver requires that the IRB or Privacy Board appropriately document that it has determined that the waiver of HIPAA authorization satisfies the following criteria:

(a) The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals based on the presence of the following elements:

1. An adequate plan to protect the identifiers from improper use and disclosure.

2. An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law (e.g., to satisfy records retention requirements).

3. Adequate written assurances that the PHI will not be reused or disclosed except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by the HIPAA Privacy Rule.

(b) The research could not practicably be conducted without the waiver.

(c) The research could not practicably be conducted without access to and use of PHI.

(d) A summary of PHI to be used or disclosed.

(e) The IRB's or Privacy Board's documentation must be signed by the Chair or other designated voting member and include the requirements of the IRB identification, date of waiver approval and review procedure used (convened or expedited).

(9) VHA personally identifiable information, including health information involving employee research subjects in their capacity as a VA employee, may be used by a VA Investigator for research purposes in accordance with VHA Directive 1200.05(3), applicable 1200 series directives and 38 C.F.R. part 16.

(10) VA Investigators conducting VHA-approved research may use a limited data set provided a DUA is obtained. Written HIPAA authorization from the subject or a waiver of HIPAA authorization is not required when a limited data set is used.

(11) A DUA may be required for research when data is transferred from a national database, VISN warehouse or a research data repository. VHA Handbook 1200.12 states the requirements for when a DUA must be used for research. The Information Custodian may choose to require a DUA before data is provided for VA research studies as a best practice.

(12) VA Investigators may use and disclose the requested data only in a manner consistent with the approved research protocol and as indicated in the written HIPAA authorization from the subject or waiver of HIPAA Authorization. When the HIPAA authorization is combined with the informed consent form, the VA Investigator may use and disclose the requested data consistent with the informed consent.

(13) VA Investigators may use personally identifiable information for potential recruitment of study subjects only if the IRB or Privacy Board has granted a waiver of HIPAA authorization for this use. ***NOTE:*** *Unless the waiver of HIPAA authorization is approved for the whole study, a HIPAA authorization must be obtained once the subject is recruited but before any other research interventions take place.* VHA Directive 1200.05(3) states other requirements that must be met for recruitment of research subjects.

(14) If a research subject properly executes a written HIPAA authorization for disclosure of their PHI to an affiliate institution or other entity, transfer of the information constitutes a "disclosure" under the Privacy Act and HIPAA Privacy Rule. Depending on the agreement between the transferring facility and the receiving entity, VA may or may not retain data ownership. Absent an agreement that restricts the affiliates or other entity's further use or disclosure of the information (e.g., contract, MOU, MOA or DUA); ownership of the disclosed data transfers to the recipient and VA cedes control over the information.

(15) Approval from the VA Area Manager or appropriate Information System Security Officer (ISSO) must be obtained before VA sensitive information, including personally identifiable information, can reside on non-VA owned equipment, such as the affiliate's servers or computers.

b. **Case Reports or Case Studies.** Case reports or case studies are not typically considered to be research, rather they are typically considered to be educational and related to clinical care. Case reports or case studies usually involve a retrospective report of the observation of one or a few patients whose novel condition(s) or response(s) to treatment was guided by the care provider's judgment regarding the best interest of the patients. De-identified information may be used by a VA employee for publication of a case study or by a VA-affiliated HPT as part of studies including in a classroom setting or thesis. Case reports or case studies shall contain only de-identified information under the specific requirements of the HIPAA Privacy Rule or pictures that totally conceal the identity of the individual. If personally identifiable information or PHI must be used, a signed, written authorization from the patient or the patient's personal representative is required. Authors of case studies or case reports must consult with the VA medical facility Privacy Officer to ensure that all information is appropriately de-identified as required by the HIPAA Privacy Rule. The VA medical facility Privacy Officer has the authority to make this final determination. ***NOTE:*** *There are some circumstances where a case report or case study may be considered as research. If there is any indication that the case report or case study may be research, the IRB or VA medical facility Research Office must be consulted*. *See VHA Directive 1200.05(3) for more guidance.*

c. **Cooperative Research and Development Agreement.** A Cooperative Research and Development Agreement (CRADA) is a written agreement between VA and one or more non-Federal parties to work together on a research project. CRADAs focus on the intellectual rights of a study (e.g., a drug patent). If a research study is being conducted under a CRADA, a DUA is not required to share VA sensitive information, as the protections of a DUA are built into the VA CRADA templates used by research staff. See VHA Directive 1206, Use of a Cooperative Research and Development Agreement (CRADA), dated June 19, 2018.

d. **Documentation.** The original informed consent and HIPAA authorization for Research involving human subjects are maintained under the Privacy Act System of Records Notice (SORN) 34VA12, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA." If copies of these documents (informed consent and HIPAA authorization) are included in the health record, then these copies are covered under the Privacy Act SORN 24VA10A7, "Patient Medical Records-VA" and are disclosed in accordance with Routine Use Disclosure Statements under that SORN. The original documents are kept with the VA Investigator's file.

e. **Release of Information for Non-VA Investigators (Extramural).** VHA has authority to disclose individually identifiable information to non-VA investigators performing non-VA research in accordance with this directive and the applicable Privacy

Act System of Records. The request must be for a specific non-VA research study with IRB approval or notice of IRB exemption.

(1) **Reviews Preparatory to Research.** A non-VA investigator, except for a Department of Defense (DoD) investigator, may not review VHA individually identifiable information preparatory to research.

(2) **Information from Research Subjects Who are Not VHA Employees.**

(a) VHA may disclose the individually identifiable health information of research subjects who are not VHA employees (e.g., Veterans, their beneficiaries, caregivers and patients) to non-VA Investigators for research purposes provided there is a prior signed, written HIPAA authorization.

(b) Disclosure to Federal Investigators (Researchers). If there is no prior signed, written HIPAA authorization, VHA may disclose individually identifiable health information to non-VA Federal investigators (researchers) (e.g., DoD, Indian Health Service) for research purposes if:

1. The research has been approved by the researcher's IRB of record and an IRB or Privacy Board has waived the requirement for a HIPAA authorization in accordance with 45 C.F.R. § 164.512(i) prior to the request for the individually identifiable health information. ***NOTE*****:** *Research activities involving PHI may be exempt from the Common Rule. Some exempt activities will require a limited IRB review. Please refer to VHA Directive 1200.05(3).*

2. There is approval by the Under Secretary for Health or designee based on the records being disclosed. For the Under Secretary of Health or designee as appropriate to approve the request, there first must be a recommendation of approval from the VHA Privacy Office and Chief R&D Officer.

3. When 38 U.S.C. § 7332-protected information is also requested, the non-VA Federal investigators must submit written assurance that the purpose for requesting data is to conduct scientific research and the requirements in 38 C.F.R. § 1.488 (see paragraph 13.e.(2)(d) below) are met. ***NOTE:*** *This assurance may be documented in the research protocol.*

4. A Certificate of Confidentiality does not prohibit the disclosure of individually identifiable health information to other Federal agencies for non-VA Federal Research.

(c) Disclosure to Non-VA, Non-Federal Investigators. If there is no prior signed, written HIPAA authorization, VHA may disclose individually identifiable health information for research purposes to non-VA, non-Federal investigators if:

1. There is a signed, written request that reasonably describes the information sought as required by 38 U.S.C. § 5702.

2. The research has been approved by the investigator's IRB of record and R&D Committee and an IRB or Privacy Board has waived the requirement for a HIPAA authorization in accordance with 45 C.F.R. § 164.512(i) prior to the request for the individually identifiable health information. ***NOTE:*** *Research activities involving PHI may be exempt from the Common Rule. Some exempt activities will require a limited IRB review. Please refer to VHA Directive 1200.05(3).*

3. There is approval by the Under Secretary for Health or designee. For the Under Secretary of Health or designee as appropriate to approve the request, there first must be a recommendation of approval from the VHA Privacy Office and Chief R&D Officer.

4. When 38 U.S.C. § 7332-protected information is also requested, the non-VA, non-Federal investigators must submit an assurance in writing that the purpose for requesting data is to conduct scientific research and the requirements in 38 C.F.R. § 1.488 (see below) are met.

5. Names and addresses of the non-employee research subjects may not be provided to the non-VA, non-Federal investigator except when the non-VA, non-Federal investigator first provides such names and addresses to VA.

6. There is a properly executed DUA.

(d) Requirements of 38 C.F.R. § 1.488. 38 U.S.C. § 7332-protected information may be disclosed without written HIPAA authorization if, in addition to the above applicable requirements, the requirements of 38 C.F.R. § 1.488 are met. Specifically, the written assurance must indicate:

1. The information must be maintained in accordance with the security requirements of 38 C.F.R. § 1.466, or more stringent requirements,

2. The information will not be re-disclosed, except back to VA, and

3. The information will not identify any individual patient in any report of the research, or otherwise disclose patient identities.

(e) Requests for a limited data set for research from non-VA Investigators must be in writing; meet all of the requirements in paragraphs 13.e.(2)(c) and 13.e.(2)(d) above with the exception of the IRB or Privacy Board having waived the requirement for a HIPAA authorization; be approved by the investigator's IRB of record, if required by applicable Federal regulations, or determined to be exempt; and an appropriate DUA must be executed prior to the disclosure of the limited data set.

(f) Requests for de-identified information from non-VA Investigators must be in writing and meet the requirements of Appendix A as well as all the requirements in paragraphs (c) and (d) above with the exception of the IRB or Privacy Board having waived the requirement for a HIPAA authorization in accordance with 45 C.F.R. § 164.512(i). An appropriate DUA must be executed prior to the disclosure of the information.

(g) If the research does not meet the definition of Human Subject Research per the Common Rule (38 C.F.R. part 16), the non-VA Investigator's institution must approve the research.

(3) **Information from Research Subjects in their Capacity as VHA Employees.**

(a) VHA may disclose the personally identifiable information of research subjects in their capacity as VHA employees, excluding health information, to non-VA Investigators for research purposes without written HIPAA authorization, and only in accordance with the Privacy Act, as appropriate, and applicable VA privacy policy. Depending on the location of the records and the System of Records in which they reside, records that contain individually identifiable health information on VHA employees may be subject to the HIPAA Privacy Rule.

(b) VHA employee health information may be disclosed for research using the same privacy processes as Veteran health information with the approval of VHA Occupational Health Services.

14. AUTHORIZATION REQUIREMENTS

a. **Written Authorization.**

(1) A written authorization signed by the individual to whom the information or record pertains is required when:

(a) VA health care facilities need to utilize individually identifiable health information for a purpose other than treatment, payment or health care operations and other legal authority to do so, as specifically noted by this directive, does not exist,

(b) VA health care facilities need to disclose information for any purpose for which other legal authority does not exist, or

(c) VA health care facilities want to conduct marketing, except when communicated face-to-face to an individual. If the marketing involves financial remuneration to the covered entity from a third party, the authorization must state that such remuneration is involved. ***NOTE:*** *Financial remuneration does not include any payment for treatment of an individual.*

(2) The written authorization must comply with all the requirements of paragraphs 14.b. through 14.h. ***NOTE:*** *Adults filing online for Social Security disability benefits on their own behalf can electronically sign and submit their "Authorization to Disclose Information to the Social Security Administration" (Form SSA-827). A third party or personal representative will not be able to electronically file an authorization on behalf of the individual. VHA accepts electronically signed and submitted Form SSA-827.*

(3) VHA may not condition the provision of treatment, payment, enrollment in the VA health care program or eligibility for benefits on the signing of an authorization, except

for research-related treatment where an authorization for the use or disclosure of individually identifiable health information for such research is required.

b. **Requirements of an Authorization to Release Information.**

(1) When an authorization of the individual is required to release personally identifiable information, the authorization must be in writing and include the following information:

(a) The identity, (e.g., full name and date or birth, mailing address) of the individual to whom the information pertains sufficient to locate the individual's records. The last four digits of the SSN may be added to the bottom of VA Form 10-5345 for scanning and filing within the Veteran's health record; however, even the last four SSN digits cannot be added to the form if the form is being mailed to the requestor.

(b) A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion. If HIV, sickle cell anemia, drug or alcohol abuse treatment information (i.e., 38 U.S.C. § 7332-protected information) is to be disclosed for purposes other than treatment, billing or those authorized by the act, this information must be specifically identified in the description. If individually identifiable information created in the future is to be disclosed, the description must indicate such.

(c) The name, or other specific identification, of the person(s), class of persons or office designation(s) authorized to make the requested use or disclosure. Generic language, such as Department of Veterans Affairs or name of VA medical facility, is acceptable.

(d) The name or other specific identification of the person(s), class of persons or office designation(s) to whom the agency may make the requested use or disclosure. Categories or classes, such as My Providers, Court staff and family members, are acceptable. Address is not required on the authorization form.

(e) A description of the purpose or need of the requested use or disclosure.

(f) An expiration date or event that relates to the individual or the purpose of the use or disclosure. For example, VA Form 10-5345 supplies three possible expiration options: 1) After one-time disclosure, if all needs are satisfied; 2) on a specified date provided by the patient; or 3) under conditions specified by the individual. "Upon satisfaction of the need for the disclosure" is only sufficient if the "purpose" section of the authorization is clearly articulated, such as insurance claim or payment of claim, to allow the facility to determine when the need has been satisfied. Examples of appropriate expiration date language are as follows:

1. The statement "end of the research study" or similar language may be defined by the investigator or study sponsor for use or disclosure of personally identifiable information. VA Form 10-0493 provides this as an expiration option.

2. The statement “none” or similar language is sufficient if the authorization is for the agency to use or disclose personally identifiable information for a research database or research repository. When the information is used in a new research study, the investigator must obtain either a new authorization for the new study or a waiver of authorization from an IRB or Privacy Board.

3. When the future use of data or specimens is included in the research protocol, VA Form 10-0493 supplies four possible options: 1) expire at the end of this research study; 2) not expire; 3) expire on the following date or event; or 4) expires at the end of the research study unless the research subject has provided additional permission to store their data or biological specimens in a research data repository or when further optional analysis of the subject's specimens has been complete.

(g) The handwritten or electronically created and authenticated signature of the individual, or the individual’s personal representative. If a competent individual is unable to physically sign due to a physical limitation or disability, see paragraph 5.a.(10).

(h) The date signed by the individual or their personal representative. The authorization shall not be pre-dated by VHA employees as the individual or the individual’s personal representative should enter the date of signature. If a competent individual is unable to enter the date, the VHA employee may enter the date and initial the entry.

(i) A statement that the individual has the right to revoke the authorization in writing except to the extent that the entity has already acted in reliance on it.

(j) A description of how the individual may revoke the authorization (i.e., to whom the revocation is provided and any requirements).

(k) A statement that treatment, payment, enrollment or eligibility for benefits cannot be conditioned on the individual completing an authorization. Participation in a research study as well as receipt of research-related treatment may be conditioned on the individual signing the authorization (see 45 C.F.R. § 164.508(b)(4)(i)). This statement is required on all VHA authorizations and on authorizations from other HIPAA covered entities requesting VHA records.

(l) A statement that personally identifiable information or individually identifiable health information disclosed pursuant to the authorization may no longer be protected by Federal laws or regulations and may be subject to re-disclosure by the recipient.

(m) Authorization may be given on VA Form 10-5345 or any HIPAA compliant authorization form or any correspondence, provided it meets all the requirements noted above in paragraph 14.b. to be considered a valid authorization.

(n) If the authorization is for VA research purposes, VA Form 10-0493 must be used when not combined with the Research Informed Consent Form. The HIPAA authorization may not be combined with the Research Informed Consent for VA research purposes when the study includes optional components involving identifiable

data or biospecimens, such as an option for the subject to place their identifiable research data into a future use research repository. When the HIPAA authorization is combined with the Research Informed Consent Form, the VA medical facility Privacy Officer has approval authority for the authorization language within the combined form. ***NOTE:*** *Photocopies, scanned documents, or faxes of authorizations forms are acceptable after the validity of the form has been verified by the ROI Department. The validation of the authorization form can be accomplished by reviewing previous wet signatures.*

c. **Invalid Authorization.**

(1) Information will not be used or disclosed based on an authorization form that:

(a) Fails to meet any of the requirements set forth in paragraph 14.b.,

(b) Has expired,

(c) The expiration event date is known to have occurred or is not listed,

(d) An expiration, condition or event is not listed,

(e) Is known to have been revoked,

(f) Has been combined with another document to create an inappropriate compound authorization (see paragraph 14.h.),

(g) Is known, or in the exercise of reasonable care would be known, to VHA personnel to be false or inaccurate with respect to any item of the authorization requirements, or

(h) Is not signed or was signed by a deceased individual. The authorization must be signed by the individual or personal representative to be valid.

(2) If an authorization form is invalid, notify the requester of the deficiencies; except those for 38 U.S.C. § 7332-protected information (see paragraph 14.f.).

d. **Who May Sign an Authorization.**

(1) Written authorization for ROI is valid when signed by:

(a) The individual.

(b) The individual’s personal representative, which includes:

1. A court-appointed legal guardian. ***NOTE:*** *A VA Federal fiduciary administratively appointed by VBA to administer a beneficiary's VA monetary benefits is not empowered to exercise privacy rights of the VA beneficiary who is the subject of that appointment including signing an authorization.*

2. A person legally authorized in writing by the individual (or the individual's legal guardian) to act on behalf of the individual (i.e., POA).

3. A person authorized by Federal, State, local or tribal law to act on behalf of a living individual.

(c) If the individual is deceased, then the executor of estate, next-of-kin, or other person who has authority to act on behalf of the deceased individual or decedent's estate.

(2) When an individual signs an authorization form, a copy of the completed signed authorization must be provided to the individual.

e. **Duration of Authorization.**

(1) An authorization for the use or disclosure of personally identifiable information is only valid for the period specified in the authorization. It is recommended for a third-party request that the expiration date does not exceed 5 years. An authorization that does not contain an expiration date, or a specified ascertainable event or condition (e.g., end of research study) that will terminate the authorization is not valid and needs to be returned to the requester for language regarding the duration of an authorization.

(2) Generally in VHA, personally identifiable information is not to be disclosed if it was created after the date the authorization was signed. However, an individual may authorize disclosure of information created after the date the authorization was signed through explicit language included to this effect in the authorization provided that the authorization encompasses the category of information that was later created, and that the authorization has not expired or been revoked by the individual. Per HHS-OCR unless otherwise expressly limited by the authorization, a covered entity may use or disclose the PHI identified on the authorization regardless of when the information was created.

(3) If an individual dies prior to executing the authorization, the authorization is not valid. When an individual dies, the authorization, if still otherwise valid, is considered immediately revoked and no longer valid.

(4) VA medical facilities cannot impose an expiration timeframe, e.g., 180 days, on third-party authorizations when an expiration date, event or condition is listed on the authorization. VA medical facilities cannot refuse to accept a signed, written authorization that meets the requirements in paragraph 14.b., is valid based on the requirements in paragraph 14.c. and unexpired. VHA has no authority to refuse to accept such an authorization or mandate another one be provided.

f. **Authorization Content Requirements for Human Immunodeficiency Virus, Sickle Cell Anemia, Drug and Alcohol Information (Special Authorization).**

(1) When a requester presents VHA with an insufficient authorization for records protected under 38 U.S.C. § 7332, VA must, in the process of obtaining a legally

sufficient authorization, correspond only with the living individual whose records are involved, or the legal guardian of the individual if the individual is incompetent, or the person who is authorized to act on behalf of the deceased individual (see paragraph 33).

(2) The requester can be contacted if the authorization is invalid to let them know that it is invalid, however they cannot be advised that individually identifiable health information relating to the treatment for or referral for drug abuse, alcoholism, or alcohol abuse, tests for or infection with HIV, or sickle cell anemia or trait is the reason the authorization is invalid.

(3) When VHA has legal authority to make a disclosure of 38 U.S.C. § 7332-protected information without a signed, written authorization (see paragraph 40.b.(4)) and the third party chooses to provide an authorization from the individual, the authorization is not required to explicitly specify the disclosure of HIV, sickle cell anemia, drug abuse or alcohol abuse. For guidance on addressing 38 U.S.C. § 7332-protected information on VA Form 10-5345, see Completion of VA form 10-5345, Request for and Authorization to Release Health Information Practice Brief at: https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/FactSheets.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

g. **Prohibition on Re-disclosure of 38 U.S.C. § 7332-Protected Information.**

(1) Whenever a known written (i.e., paper or electronic) disclosure of 38 U.S.C. § 7332-protected information is made with the individual's signed, written special authorization, the disclosure must be accompanied by the following or similar written statement:

"This information has been disclosed to you from records protected by Federal confidentiality statute 38 U.S.C. 7332. Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written authorization of the person to whom it pertains or as otherwise permitted by 38 U.S.C. 7332. A general authorization for the release of medical or other information is not sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any human immunodeficiency virus, sickle cell anemia, or alcohol or drug abuse patient."

(2) Whenever a known written disclosure of 38 U.S.C. § 7332-protected information is made pursuant to 38 U.S.C. § 7332(b)(2)(H) for purposes of providing health care to patients, the disclosure must be accompanied by a notification to the entity to which the record is disclosed that the record may not be disclosed or used for a purpose other than that for which the disclosure was made or as permitted by law.

(3) VHA is not required to review all the individually identifiable health information being disclosed pursuant to a signed, written special authorization or for treatment purposes in order to ascertain and know whether 38 U.S.C. § 7332-protected information is included in the disclosure.

h. **Compound Authorizations.**

(1) A compound authorization is one in which an authorization for the use or disclosure of PHI is combined with other legal written permission. An authorization for use or disclosure of PHI may not be combined with another document to create a compound authorization, except as follows:

(a) An authorization for a research study may be combined with any other type of written permission for the same or another research study, including combining an authorization for a research study with the informed consent or another authorization for the same research study or with an authorization for the creation or maintenance of a research database or repository, and

(b) An authorization may be combined with any other authorization, except when VHA has conditioned the provision of treatment, payment, enrollment in a health plan or eligibility for benefits on the provision of one of the authorizations.

(2) Where VHA has conditioned the provision of research-related treatment on the provision of one of the authorizations, any compound authorization created must clearly differentiate between the conditioned/mandatory and unconditioned/optional components and provide the individual with an opportunity to explicitly opt into the research activities described in the unconditioned/optional section of the compound authorization under separate signature. ***NOTE:*** *VA Investigators are not required to combine HIPAA authorizations or combine HIPAA authorizations with the Informed Consent Forms for the research study. Separate HIPAA authorizations may be used.*

i. **Written Requests for Personally Identifiable Information.**

(1) Requests for copies of records or written information maintained by VA must be in writing per 38 U.S.C. § 5702 and 38 C.F.R. § 1.526, Copies of Records and Papers, which states, “Any person desiring a copy of any record or document in the custody of the Department of Veterans Affairs, must make written application for such copy to the VA installation having custody on the subject matter desired stating specifically: (1) The particular record or document the copy of which is desired… and (2) the purpose for which such copy is desired to be used.”

(2) Veterans making a first party right of access request in writing as outlined in paragraph 7 satisfies this requirement.

(3) A written request is required from an outside entity wanting copies of VA records even when an authorization to permit the disclosure is not needed. For example, even though an authorization is not required to disclose copies of PHI to a non-VA provider for treatment purposes, a written request is required and is used for accounting of disclosure purposes.

(4) A written request must provide enough information to verify who the requestor is, determine the purpose of the request, locate the records requested and determine if VHA has the authority to disclose the information requested. ***NOTE:*** *There are no*

signature requirements for a third-party requestor to sign their request for health records as long as all requirements of an accounting of disclosure can be met. Therefore, a written request from a third party may be provided via email.

(5) Exceptions to requiring the written request when providing copies of VA records:

(a) VA initiates the disclosure or release, such as providing records to health care providers when patients are referred for outside care or providing patients with discharge instructions or lab results.

(b) VA employees obtaining copies of records in the performance of their official duties.

(c) VA records are disclosed verbally to an outside entity and a written request is not required to provide disclosure authority.

(d) Disclosure of records is made pursuant to a MOA, MOU or DUA.

15. PROCESSING A REQUEST

a. **General.**

(1) Anyone may request VHA to disclose any record. Any request for information maintained in VA records must be processed under all applicable disclosure and confidentiality statutes, and regulations.

(2) The request must be in writing and describe the record(s) sought so that VHA may locate the record(s) in a reasonable amount of time.

(3) If the requester is the individual to whom the records pertain and the records are part of a Privacy Act System of Records, the policy regarding individual's right of access under paragraph 7 must be followed. If the records are not in a Privacy Act System of Records, the request must be processed under FOIA and VHA Directive 1935.

(4) If the requester is someone other than the individual to whom the record pertains (non-Federal third party), VHA must determine what information is being requested in the paragraphs below.

(a) If the record requested does not contain individually identifiable information or PHI, the request is referred to the Facility FOIA Officer for processing of the request under the FOIA and VHA Directive 1935.

(b) If the record requested contains individually identifiable information or PHI, the applicable paragraphs of this directive (paragraphs 16-34) must be reviewed for guidance concerning processing requests from the specific requester or purpose. For example, for a request from a member of Congress, see paragraph 18.

(c) If the record requested contains individually identifiable information or PHI and the guidance in paragraphs 16 and 18-34 is not applicable to the request, the request must be processed by reviewing the applicable Federal privacy laws and regulations as indicated in paragraph 17. If there is not explicit disclosure authority to permit release under Federal privacy laws, then process the request as a FOIA request.

(d) If the request is for records related to a deceased individual, the request must be processed in accordance with paragraph 34.

(5) If the requester is a Federal agency and the record requested contains personally identifiable information, the applicable paragraphs of this directive (paragraphs 16-34) must be reviewed for guidance concerning processing requests from the specific Federal requester or purpose. If the requested disclosure is not covered under paragraphs 16-34, the Facility Privacy Officer or the VHA Privacy Office must be contacted for assistance.

(6) Requests from a third party, who is not a Federal agency, for individually identifiable information or PHI must be processed within the required time standards outlined in paragraph 15.b. and the applicable fees outlined in paragraph 15.c. must be charged if an appropriate authority has been identified to allow the disclosure.

(7) A third party may request VHA to disclose or provide personally identifiable information using electronic storage media, such as on compact disk (CD), in lieu of paper copies. When the records requested exist electronically and can be reproduced in the request format, VHA must accommodate such a request. ***NOTE:*** *If a request for individually identifiable information or PHI is not clearly identified within this directive, contact the Facility Privacy Officer for assistance.*

(8) **Information Blocking Exceptions.**

(a) Refusal by VHA, as a health care provider, to exchange, disclose or provide access to PHI to a third party due to prohibitions or restrictions within applicable Federal privacy laws and regulations or application of FOIA Exemptions is not information blocking because a precondition is not satisfied. VHA is required by Federal privacy laws or regulations to satisfy a precondition, in other words obtain an authorization or have disclosure authority under the law, prior to providing access, exchange or disclosure of electronic PHI.

(b) Refusal by VHA, as a health care provider, to disclose or provide PHI to a third party because of infeasibility due to segmentation issues or other circumstances is not information blocking. Segmentation issues exist when VHA cannot fulfill the request for access, exchange or disclosure of electronic PHI because VHA cannot unambiguously segment the requested electronic PHI. Infeasibility due to other circumstances exist when VHA demonstrates through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of certain factors that led to its determination that complying with the request would be infeasible under the

circumstances. VHA must provide a written response to the requestor within 10 business days of receipt of the request with the reason(s) why the request is infeasible.

b. **Time Standards.**

(1) Requests for copies of individually identifiable information, including health information, must be answered within 20 business days from the date of receipt. The date of receipt is the date the request was received by the VA health care facility department or employee able to process the request. All requests must show the date received whether by use of a date stamp, writing the date received on the request, or entering the request in the ROI Plus software on the same day as received in person or mail.

(2) When, for good cause shown, the information cannot be provided within 20 business days from the date received, the requester must be informed in writing as to the reason the information cannot be provided and the anticipated date the information will be available not to exceed an additional 20 business days.

(3) Any requests for copies of individually identifiable health information from the individual to whom the records pertain must be processed within the timeframes indicated under paragraph 7.

c. **Fees.**

(1) **Photocopying Charges.** A fee will not be charged for any search or review of a record under the procedures addressed in this directive. Fees that may be charged to requesters in connection with processing FOIA requests are addressed in VHA Directive 1935. Upon request, the individual to whom a record pertains must be provided with one free copy of their VA Benefits record or health record information. When charges are made for additional copies of records, the fee as stated in 38 C.F.R. § 1.577(e) or subsequent regulations will be charged. However, VA medical facilities are not required to collect fees that are under $25.00.

(2) **Table of Fees.** See 38 C.F.R. § 1.561(f) for summary of chargeable fees for each category of requester. ***NOTE:*** *This only applies if fees exceed $25.00. Actual direct cost is calculated by determining the cost of operating the duplication equipment and the cost of the employee's time (base hourly rate of pay plus 16% multiplied by number of hours). Actual direct cost does not include the overhead cost of operating the facility or building, including utilities, where the equipment is located.*

d. **Requests for Information Requiring Referral to Chief Counsel.** The following types of requests for information must be reviewed with the Office of the Chief Counsel in the District, and any ROI will be made only in compliance with the instructions of Chief Counsel:

(1) Requests for medical information that is to be used in suits against the U.S. Government or in a prosecution against a patient, whether the prosecution has been instituted or is being contemplated.

(2) Subpoenas for health records issued by or under the auspices of a court or quasi-judicial body that are not accompanied by an authorization from the patient must be referred to Chief Counsel to determine whether a disclosure is necessary to prevent the perpetration of fraud or other injustice in the matter before the court. This is a regulatory requirement and cannot be waived per 38 C.F.R. § 1.511(c)(3).

(3) Requests for information that indicate possible third-party liability for the cost of hospitalization and medical services (such as tort-feasor, worker's compensation or other third-party cases) must be brought to the attention of the facility Business Office for determination whether a lien should be initiated prior to disclosure of the information. For more information, see VHA Community Care Business Office (CBO) Procedure Guide, Federal Workers' Compensation Reasonable Charges and Billing, at: https://vaww.vrm.km.va.gov/system/templates/selfservice/va_kanew/help/agent/locale/en-US/portal/554400000001031/content/554400000050620/Section-H-Federal-Workers-Compensation-Reasonable-Charges-and-Billing. ***NOTE:*** *This is an internal VA website that is not available to the public.*

16. RELEASE OF INFORMATION WITHIN VA FOR PURPOSES OTHER THAN TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS WITHOUT AUTHORIZATION

a. This paragraph covers the use and disclosure of personally identifiable information from VHA records to VA or VHA entities that may be made without signed, written authorization from the individual who is the subject of the information when the purpose is other than treatment, payment or health care operations. This paragraph does not encompass every possible use or disclosure made from VHA records to VA or VHA entities. An accounting of these uses or disclosures is not required.

b. **Veterans Benefits Administration.**

(1) VHA may disclose Veteran's personally identifiable information to VBA for eligibility for, or entitlement to, or to provide benefits under the laws administered by the Secretary of Veterans Affairs (see 45 C.F.R. § 164.512(k)(1)(iii)). Such benefits include adjudication of VA benefit claims and entitlement to VA health care.

(2) VHA may disclose all other non-Veteran VHA records or information to VBA for any official purpose authorized by law.

c. **Board of Veterans Appeals.** VHA may disclose Veteran personally identifiable information to BVA for eligibility for, or entitlement to, or that provide benefits under the laws administered by the Secretary of Veterans Affairs (see 45 C.F.R. §164.512(k)(1)(iii)). ***NOTE:*** *Such benefits include processing adjudication of claims on appeals.*

d. **National Cemetery Administration.** VHA may disclose personally identifiable information to NCA for eligibility for, or entitlement to, or that provide benefits under the laws administered by the Secretary of Veterans Affairs (see 45 C.F.R. §

164.512(k)(1)(iii)). For example, VHA may provide NCA claimant information for burial benefits.

e. **VA Office of Employment Discrimination, Complaints and Adjudication.**

(1) The VA Office of Employment Discrimination, Complaints and Adjudication (OEDCA) reviews the merits of employment discrimination claims filed by present and formal VA employees and non-agency applicants for employment.

(2) VHA may disclose personally identifiable information to OEDCA when necessary for determining compliance with Equal Employment Opportunity (EEO) requirements.

f. **VA Office of Inspector General.**

(1) VA OIG provides independent advice and objective reporting to the Secretary of Veterans Affairs as well as Congress. VA OIG investigates criminal activity waste, abuse, mismanagement, safety issues and violations of law.

(2) VHA must provide any information, including personally identifiable information, to VA OIG for any official purpose authorized by law. The individually identifiable health information includes 38 U.S.C. § 7332-protected information for the purpose of health oversight (see 45 C.F.R. § 164.512(d)). Unless otherwise specified by VA OIG, all requests for VHA individually identifiable health information shall be considered as health oversight activities. In general, criminal investigative activities not related to health care fraud are treated as law enforcement activity and not health oversight. VA OIG is not required to provide VHA with a formal written request for health oversight activities; however, the OIG Investigator is required to make the request in writing (e.g., email) and to indicate the disclosure is for health oversight. The Facility Privacy Officer may ask for clarification if the request appears to be for law enforcement activities.

(3) For guidance on disclosures to VA OIG for purposes of law enforcement activities, see paragraph 21.i. on VA Police and VA OIG (see 45 C.F.R. § 164.512(f)). VHA requires a written request for those disclosures made for the purpose of law enforcement criminal investigations that involve the disclosure of PHI.

g. **VA Office of Resolution Management.**

(1) The VA Office of Resolution Management Diversity and Inclusion (ORMDI) promotes discrimination free environment focused on serving employees by preventing, resolving and processing workplace disputes in a timely and effective manner.

(2) VHA may disclose personally identifiable information to ORMDI when necessary for determining compliance with EEO requirements. VHA EEO Counselors must not place individually identifiable health information into an EEO case file without legal authority. Individually identifiable health information on Veterans must not be taken from an employee unless the employee has authority to provide the Veteran information.

h. **VHA Office of Medical Inspector.** VHA OMI typically accesses PHI for health care operations. However, when VHA OMI conducts reviews at the direction of the Secretary of Veterans Affairs to address an OSC inquiry, the reviews are for health oversight and must follow the HIPAA Privacy Rule provisions on health oversight activities. VHA must provide any personally identifiable information and 38 U.S.C. § 7332-protected information to VHA OMI for their health oversight reviews. VHA OMI is not required to provide a written request.

i. **VA Contractors.**

(1) VHA may disclose non-Veteran personally identifiable information to a VA contractor for the purposes of fulfilling the VA contract. The legal and policy requirements outlined in this directive for VA personnel to use the non-Veteran personally identifiable information apply to the VA contractor.

(2) The Facility Privacy Officer must be contacted prior to the release of any Veteran personally identifiable information to a VA contractor to ensure appropriate authority is in place.

(3) All contracts must contain the appropriate privacy and security language. See VA Handbook 6500.6, Contract Security, dated March 12, 2010. The Facility Privacy Officer collaborates with the VA medical facility ISSO and Contracting Office Representative (COR) on all contracts, new or revised.

(4) All contracts that provide for the maintenance of information in a System of Records on behalf of VA to accomplish a Department function, or provide for the disclosure of information from a VA System of Records to the contractor, must include wording that makes the provisions of the Privacy Act apply to the contractor. Such notifications and clauses must conform to those prescribed by Federal Acquisition Regulations (FAR), and VA Acquisition Regulations. VA health care facilities must comply with these requirements.

(5) When a contract provides for access to, or maintenance of, information protected by other confidentiality statutes (e.g., 38 U.S.C. §§ 5705 and 7332), the contract must provide notification to the contractor that the records are protected by these confidentiality provisions and the implementing regulations which restricts the disclosure of the information and the purposes for which the information may be used.

(6) A nursing home with which VHA has a contract may be provided personally identifiable information including health information for the purpose of fulfilling the contract for providing health care to Veterans housed in its facilities.

j. **VA Human Resources Management Services.**

(1) VHA may disclose personally identifiable information to VA Human Resources Management Services (HRMS) as authorized by law.

(2) There is no authority under the HIPAA Privacy Rule for the disclosure of a VA employee Veterans' health record to management or personnel officials for disciplinary investigation purposes without prior signed, written authorization from the employee.

(3) Employee Occupational Health (EOH) staff may not use Veteran health information for any purpose other than treatment of the employee without a signed, written authorization from the individual.

(4) VHA may disclose individually identifiable health information of non-employees to VA HRMS only for the purpose of managing the VHA work force under a Business Associate relationship.

k. **VA Police Service.**

(1) VHA may provide VA Police Service with personally identifiable information as necessary to carry out functions related to treatment or security of individuals. Security functions include issuing employee badges, securing VA premises and escorting certain individuals to their VA medical facility appointments, searching for missing Veterans or subduing Veterans. No special request or other documentation is needed.

(2) VHA may disclose personally identifiable information for purposes of law enforcement activities such as issuing parking tickets or speeding tickets on the premises; responding to auto accidents; responding to suspected criminal activity (e.g., theft from the retail store); and reporting fugitive felons (see VHA Handbook 1000.02, VHA Fugitive Felon Program, dated February 23, 2012) seeking care from the VA medical facility. For these law enforcement functions, the facility VA Police Service must follow policies outlined in paragraph 21.

(3) VHA may provide VA Police Service with personally identifiable information regarding a serious and imminent threat to the health or safety of an individual (e.g., employee) or the public (e.g., bomb threat) as long as VA Police Service is reasonably able to prevent or lessen the threat.

(4) Disclosure of personally identifiable information from VA Police Records may be made only in accordance with Federal privacy and confidentiality statutes and regulations, as well as disclosure under the VA Police System of Records (103VA07B).

(5) The VA Police Chief, or designee, must only be given minimum access to the EHR, such as to the Patient Inquiry Option in VistA. Access to CPRS by VA Police Service is not appropriate. If PHI about an individual is needed for law enforcement purposes, VA Police Service must follow the requirements of paragraph 21 and should contact the VA medical facility Privacy Officer for assistance.

l. **VA Researchers.**

(1) VHA may use employee information, including health information for official VHA research studies, in accordance with VHA Directive 1200.05(3) and 38 C.F.R. part 16.

(2) For use or disclosure of individually identifiable health information involving non-employee research subjects, such as Veterans, for research purposes, see paragraph 13.

m. **Unions.**

(1) VA unions, in the course of fulfilling their representational responsibilities, may make a request to management to provide copies of facility records pursuant to its authority under 5 U.S.C. § 7114(b)(4). Unions may request any records that are maintained by a VA health care facility. This might include releasable portions of completed Administrative Boards of Investigation (ABI), patient health records or an employee's personnel records. However, under certain circumstances, unions may not be legally entitled to receive individually identifiable health information or information protected by other statutes, such as the Privacy Act.

(2) There is no specific format that must be used by a union to make a request for agency information or records from management. Generally, a union makes a written request for "information" citing 5 U.S.C. § 7114(b)(4) or citing a particular Article or Section of the union contract. Some unions request documents or information citing the provisions of FOIA or without citing any particular statutory or contractual provision.

(3) Regardless of the format of the request, upon receipt of a request by a union for facility records, the servicing Human Resources Management (HRM) office and the Chief Counsel's office must be contacted immediately. The Chief Counsel's office must assist management officials in determining whether facility records (or information from agency records) are exempt from release pursuant to Federal law and regulations. HRM and Chief Counsel staff can refer to VHA Directive 1935 for guidance in how to process union requests for information or agency records.

17. GENERAL RELEASE OF INFORMATION OUTSIDE VA

a. **Disclosure with Authorization.**

(1) When VHA receives a request for personally identifiable information that is accompanied by a written authorization signed by the individual to whom the records pertain, disclosure needs to be made in accordance with the authorization once it has been determined that the authorization is valid. An accounting of the disclosure will be required.

(2) Disclosure is mandatory when a valid, written authorization signed by the individual is provided directly to VA by the individual or a third party. Information that is disclosed must be limited to the information that is needed to satisfy the purpose of the request.

(3) Disclosure is allowed when a valid, written authorization signed by the individual is obtained from the individual by VA, such as a Research HIPAA Authorization, but is not mandatory.

b. **Disclosure without Individual's Authorization.**

(1) This directive covers the disclosure of personally identifiable information (including health information) to entities outside VA, where prior signed, written authorization is not always needed. To the extent possible, this directive identifies the disclosure policies involving specific entities (e.g., courts, Congress and Federal or State agencies).

(2) If VHA receives a request or wishes to make disclosure to an entity outside VA that has not been identified in this directive, the VHA official processing the disclosure needs to analyze whether VHA has lawful authority to make the disclosure. Before making a disclosure of any personally identifiable information (including health information) to an outside entity, VHA needs to determine the type of information involved and the confidentiality statutes and regulations that apply to the information. The following six questions determine the type of information involved:

(a) Is the information about treatment or referral of a Veteran for drug abuse, alcohol abuse or alcoholism, sickle cell anemia or treatment for HIV infection protected by 38 U.S.C. § 7332?

(b) Is the information about the disclosure of a name or address of a present or former member of the Armed Forces and their dependents protected by 38 U.S.C. § 5701?

(c) Is the information a quality assurance review record protected by 38 U.S.C. § 5705?

(d) Is the information individually filed and retrieved by VA by an individual name or other unique identifier protected by the Privacy Act, 5 U.S.C. § 552a?

(e) Does the information involve health information protected by the HIPAA Privacy Rule?

(f) Is the information not protected by any privacy law or regulation and must be referred for processing under FOIA, 5 U.S.C. § 552?

(3) VHA needs to determine whether legal authority exists under each of the applicable statutes and regulations. For example, if the information is protected by the Privacy Act, there must be Privacy Act disclosure authority, such as a published routine use in the applicable Systems of Records authorizing the disclosure. If the disclosure authority does not exist in all applicable statutes and regulations, VHA may not make the disclosure.

(4) Disclosure is not mandatory under these provisions; however, in situations where FOIA also applies to the request, disclosure is mandatory unless a FOIA exemption applies. See VHA Directive 1935 for more detailed guidance. Information that is disclosed will be limited to the information that is needed to satisfy the purpose of the request.

c. **Required by Law Exception.**

(1) VHA may use individually identifiable health information to the extent that such use is necessary to gather or collect information for disclosure mandated or required by law and the use complies with, and is limited to, the relevant requirements of such law (e.g., gunshot wounds, adult abuse, public health reporting).

(2) VHA may disclose individually identifiable health information without an individual's signed, written authorization when mandated or required by law (e.g., statute, regulation, FOIA, court order) and when there is appropriate authority under Privacy Act and the 38 U.S.C §§ 5701 and 7332, if applicable.

(3) **Child Abuse Reporting.** VHA is permitted under applicable Federal privacy laws to report, as directed by VA policy, any incident of child abuse as required by the Victims of Child Abuse Act, 34 U.S.C. § 20341, and the Victims of Child Abuse Act Reauthorization Act of 2018, P.L. 115-424. See VHA Directive 1199(2), Reporting Cases of Abuse and Neglect, dated November 28, 2017.

18. CONGRESS

a. **Constituent Service Request - Member Acting in an Individual Capacity on Behalf, and at the Request, of the Individual to Whom the Information Pertains.**

(1) **Constituent Service Request.** A constituent service request is an inquiry from a Member of Congress on behalf of a constituent. A constituent is the individual who is requesting the Congress Member's assistance.

(a) When a constituent service request is received, VHA may disclose personally identifiable information, excluding 38 U.S.C. § 7332-protected information, to a Member of Congress or staffer in response to an inquiry made pursuant to a constituent request. The request from the congressional office must be in writing and signed. The request for information must also include a copy of the constituent's inquiry to the Member of Congress unless a signed, written authorization is provided. The applicable routine use in many VA Privacy Act systems of records permits disclosure "in response to an inquiry from the congressional office made at the request of that individual." Both the Privacy Act and HIPAA Privacy Rule permits disclosure to a Member of Congress without a signed, written authorization from the individual (Refer to the Privacy Act System of Records 24VA10A7 "Patient Medical Records-VA," Routine Use number 7 and 45 C.F.R. § 164.510(b)).

(b) If a prior signed, written authorization is provided by the constituent, the authorization must conform to the requirements of a valid authorization as described in paragraph 14.b.

(2) **Required Elements.** Before disclosing any information to a Member of Congress, and in order to confirm that the request is, in fact, an inquiry from the individual to whom the information pertains, VHA will require the following:

(a) Constituent's full name,

(b) Signature on the constituent's request letter, and

(c) At least one of the following: contact information (e.g., address, telephone number), date of birth, SSN or claim number (if different from SSN).

(d) If the constituent letter is not signed, or if other appropriate identifiers are not included, VHA may contact the constituent to confirm the legitimacy of the letter.

(3) **Requests Made by Personal Representatives.** If the constituent's inquiry is from the personal representative of the individual to whom the information pertains, VHA will require a POA, guardianship document, or some other document that demonstrates that the requester is authorized under Federal, State, local or tribal law to act on behalf of the individual. If the constituent cannot be identified with reasonable certainty with the information provided, VHA may request additional information before the request is processed.

(4) **Form or Format of Correspondence.** The correspondence from the constituent to the Member of Congress may be in the form of a letter, fax or email, provided that it contains the information required, as outlined in paragraph 18.a.(2). The correspondence must have been submitted by the individual to whom the information pertains or by their personal representative.

(a) Reports of contacts from staffers documenting telephone inquiries will not be accepted, as they are subject to error and misinterpretation.

(b) A written request must be signed by the requester who is the Congress Member or staffer per 38 U.S.C. § 5702. An attached email from the constituent does not require a signature unless it is used as one of the required elements.

b. **Oversight Request - Member of a Congressional Committee or Subcommittee for Oversight Purposes.**

(1) VHA may disclose personally identifiable information to a committee or subcommittee of Congress having oversight jurisdiction of VA activity to which the information pertains, without the record subject's prior signed, written authorization, provided that the Chair of the committee or subcommittee makes the request, in writing, on behalf of the Committee or Subcommittee, (e.g., House and Senate Committees on Veterans Affairs, House Committee on Oversight and Government Reform, Senate or House Appropriations Committees, Senate Committee on Homeland Security and Government Affairs) on committee letterhead for committee or subcommittee oversight functions.

(a) When personally identifiable information is provided, the VHA official providing the information must advise the committee or subcommittee, in writing, that the information is being released for official purposes only and that given its private, confidential nature, the information needs to be handled with appropriate sensitivity.

(b) If the request by the member is for any purpose other than oversight, the VHA official processing the request must do so in accordance with the guidance provided in paragraphs 18.a. or 18.c.

(c) Communications from the committee ranking minority members, other Members of Congress or staff members do not qualify as oversight requests but are acceptable for the purpose of clarifying an original oversight request as long as the subsequent communications does not expand the scope of the original request.

(d) VA may provide information sought to another member or a staffer, if specifically requested to do so by the Chair.

(2) VHA may disclose 38 U.S.C. § 7332 to a Congressional committee upon written request for program oversight and evaluation if such records pertain to any matter within the jurisdiction of such committee or subcommittee (see 38 C.F.R. § 1.489(c)).

c. **Member of Congress Acting on Behalf of a Third Party.**

(1) VHA may not disclose individually identifiable information upon an inquiry from a Member of Congress on behalf of a third party (e.g., spouse, family member, friend) unless the third party has provided a properly executed prior signed, written authorization from the patient or the third party is the personal representative of the individual to whom the information pertains.

(2) If the third party does not provide such authorization, the responding VHA official must advise the Member of Congress that the written authorization of the individual about whom the information pertains is required before VHA may disclose the information requested.

19. CONSUMER REPORTING AGENCY

a. VHA may disclose individually identifiable information, including health information, but excluding 38 U.S.C. § 7332-protected information, to consumer reporting agencies, including credit reporting agencies, for purposes of assisting in the collection of indebtedness to VA provided that the provisions of 38 U.S.C. § 5701(g)(4) have been met.

b. Information may be released concerning an individual's indebtedness to a consumer reporting agency for the purpose of making information available for inclusion in consumer reports regarding the individual, if VA, in accordance with 38 C.F.R. § 1.900-1.970, has:

(1) Made reasonable efforts to notify the individual of the individual's right to dispute, through prescribed administrative processes, the existence or amount of such indebtedness and of the individual's right to request a waiver of such indebtedness under 38 U.S.C. § 5302,

(2) Afforded the individual a reasonable opportunity to exercise such rights,

(3) Made a determination with respect to any such dispute or request, and

(4) Allowed 30 calendar days to elapse following the day that VA made a determination that reasonable efforts have been made to notify the individual that VA intends to release the information for such purpose.

20. COURTS, QUASI-JUDICIAL BODIES AND ATTORNEYS

a. **Court Orders.**

(1) Individually identifiable health information may be disclosed pursuant to a Federal, State or local court order when accompanied by a written authorization signed by the individual of the records involved, or by the individual's legal representative. If the records contain 38 U.S.C. § 7332-protected information, the written authorization must comply with the requirements set forth in 38 C.F.R. § 1.475 and specifically give permission to disclose 38 U.S.C. § 7332-protected information.

(2) VA may disclose health records pursuant to an order from the court of competent jurisdiction without written authorization, under 5 U.S.C. § 552a(b)(11) and 45 C.F.R. § 164.512(e). "Competent jurisdiction" means a judicial official with the authority to enforce the order (e.g., by holding a VA official in contempt of court for not producing the record). Orders issued by administrative bodies such as the Equal Employment Opportunity Commission, Merit Systems Protection Board or other administrative bodies are not considered to be orders from a court of competent jurisdiction providing VA with the necessary disclosure authority under the Privacy Act's court order exception. See "Quasi-Judicial Bodies" below.

(3) **Federal Court Order.** Individually identifiable information will be released for use in proceedings in a Federal court in response to a court order in accordance with 38 C.F.R. § 1.511 and 38 C.F.R. §§ 14.800-14.810. When the request is not on behalf of the U.S., the cost of producing and reproducing the records, as well as the cost for a VA employee to appear in court to present the records, must be paid in advance. Such fee must be sent to the U.S. Treasury by VA in accordance with established procedures.

(4) **State or Local Court Order.** Individually identifiable information may be released for proceedings in State or local courts in response to a court order. Without an authorization from the individual, an affidavit from the attorney requesting the information or records may be required by Chief Counsel to ascertain that disclosure of these records is necessary to prevent the perpetration of fraud or other injustice in the matter before the court. Any requests for documents or records for a use clearly adverse to the subject of the records (e.g., subject is defendant in a VA lawsuit) must be referred to Chief Counsel. This is a regulatory requirement and cannot be waived per 38 C.F.R. § 1.511(c). Contact the appropriate Chief Counsel regarding when such an affidavit is required.

(a) The affidavit must state:

1. The character of the proceedings, and

2. The purpose for which the requested information or records are to be used in evidence.

(b) If the order includes information that is sufficient to serve the purpose of the affidavit, an affidavit is not required.

(c) The person who obtained the court order or subpoena, issued or approved by a judge of the court, must be furnished requested copies of the information or record after payment of the proper fee.

(5) When a disclosure is made in response to a court order without the written authorization of the individual, the VA health care facility must send a written notice of that disclosure to the last known address of the individual whose records were disclosed.

b. **Subpoenas.**

(1) A subpoena does not provide the sufficient authority under the Privacy Act to disclose individually identifiable information, including health information, unless the subpoena is signed by a court of competent jurisdiction or the judge of a court of competent jurisdiction, or it is accompanied by the signed, written authorization of the individual whose records are the subject of the subpoena. This applies to Federal, State, municipal and administrative agency subpoenas.

(2) When a subpoena for individually identifiable information is received, which is not signed by a court or judge or accompanied by the signed, written authorization of the individual, the Chief Counsel or upon advice from the Chief Counsel the Facility Privacy Officer or designee must notify the party responsible for the issuance of the subpoena that VHA is not authorized to disclose the information in response thereto. They must be advised that for VHA to have disclosure authority with regard to such subpoenaed information, the requester must have the written authorization of the specific individual, a court order or a request that complies with other applicable authority under law (i.e., law enforcement request).

(3) When personally identifiable information is subpoenaed but the Privacy Act does not apply (e.g., the subject of the records is deceased, is not a U.S. citizen and does not reside in the U.S., VA does not retrieve the record by the name of the record subject or another identifier assigned to that individual, or data is deidentified in accordance with this directive), VHA may disclose records, excluding 38 U.S.C. § 7332-protected information. Chief Counsel must be contacted before disclosure to ensure any 38 U.S.C. § 5701 information is necessary to prevent the perpetration of fraud or other injustice before the court.

(4) When a disclosure of PHI is made in response to a subpoena without the signed, written authorization of the individual, the VA health care facility is required to send a written notice of that disclosure to the last known address of the individual whose records were disclosed. ***NOTE:*** *Federal and State court orders and subpoenas cannot be ignored even if one determines that VA has no lawful authority to disclose. Federal*

and State courts can still seek to enforce an order or a subpoena through contempt proceedings against the specific individuals responsible for the records. As soon as a VA health care facility receives an order or a subpoena, the VA health care facility must immediately contact Chief Counsel for guidance.

c. **Quasi-Judicial Bodies.**

(1) VA may disclose any personally identifiable information to a quasi-judicial body in accordance with Federal policy and applicable law. A quasi-judicial body is an individual or organization that has powers resembling those of a court of law or judge and is able to remedy a situation or impose legal penalties on a person or organization. Quasi-judicial activity is limited to the issues that concern the particular administrative agency (e.g., Social Security Administration (SSA), Federal Merit Systems Protection Board, Equal Employment Opportunity Commission and State workers' compensation boards).

(2) An order from a Federal or State quasi-judicial agency is not a court order and does not provide disclosure authority under the Privacy Act court order exception. VA may disclose if the request qualifies as a law enforcement request, a Privacy Act routine use permits disclosure, the individual provides written authorization or the agency obtains a qualifying court order.

(3) Absent a special court order, quasi-judicial bodies must obtain the signed, written authorization of the patient to obtain 38 U.S.C. § 7332-protected information.

d. **Attorneys.** Direct requests from attorneys for copies of individually identifiable information for use in litigation must be accompanied by the signed, written authorization of the individual.

e. **Producing Individually Identifiable Information In Person in Court or Quasi-Judicial Proceedings.**

(1) Original VHA records must remain in the custody of a VA employee at all times. An employee who brings records to a judicial proceeding must promptly report their presence to the Clerk of the Court. The employee may be requested to take the witness stand but will limit testimony to identification of the record as custodian of the record and must not comment on the content of the record.

(2) Original VHA information or records must never be relinquished (i.e., physically turned over) to courts or quasi-judicial bodies. For paper records, it is advisable to prepare a photocopy of the information or record. For electronic records, such as those in EHR, a printed copy of the electronic records is not the original. If the judge or the attorney requests the entire or part of the original paper record to be held in evidence, permission needs to be obtained to substitute the copy so that the original remains in VA custody. ***NOTE:*** *If the court insists on retaining the original paper records or any portion thereof, Chief Counsel must be contacted immediately for assistance.*

(3) When a VHA employee is requested to testify to the facts contained in the record and the facts are within the employee's knowledge, a determination must be made as

provided in 38 C.F.R. § 1.522 whether disclosure of any facts or information would be detrimental to the physical or mental health of the individual. When the record contains information that has been determined injurious to the individual, the employee must ask the court that the contents of the record not be disclosed, and that the employee not be required to testify.

(4) VA health care facilities must develop procedures related to employees presenting testimony or VHA records in court. The assistance of the Chief Counsel must be requested in developing these procedures to ensure compliance with VA regulations and State requirements.

f. **Personally Identifiable Information Protected by 38 U.S.C. § 7332.**

(1) **Legal Effect of Court Order.**

(a) Personally identifiable information or records that relate to treatment for drug abuse, alcoholism or alcohol abuse, sickle cell anemia or treatment for HIV may be disclosed if authorized by an appropriate order of a court of competent jurisdiction (Federal, State or local) under the provisions of 38 C.F.R. § 1.490. An application for a court order must use a fictitious name such as "John Doe" to refer to any individual. A subpoena is not sufficient authority to authorize disclosure of these records. An order requiring a disclosure that is issued by a Federal court compels disclosure of the information record. However, such an order from a State or local court only acts to authorize the VA health care facility to exercise discretion to disclose the records.

(b) In assessing a request to issue an order, the court is statutorily required to weigh the public interest and the need for disclosure against the injury to the patient, to the provider-patient relationship and to the treatment services. To assist the court in weighing the interests involved in deciding whether to issue a court order, a VA health care facility, after consultation with Chief Counsel, may provide the court expert evidence from VA health care providers explaining the effect a court order could have on an individual's privacy, the patient-provider relationship and the continued viability of the treatment program. Upon granting an order, the court, in determining the extent to which any disclosure of all, or any part, of any record is necessary, is required by statute to impose appropriate safeguards against unauthorized disclosure (see 38 U.S.C. § 7332(b)(2)(D)). A Federal, State or local court order to produce records is not sufficient, unless the order reflects that the court has imposed appropriate safeguards to protect the information from unauthorized disclosures (see 38 C.F.R. § 1.493(e)).

(2) **Information Obtained for Research, Audit or Evaluation Purposes (Non-treatment).** A court order may not authorize any person or entity that has received 38 U.S.C. § 7332-protected information from VHA for the purpose of conducting research, audit or evaluation to disclose this information in order to conduct any criminal investigation or prosecution of an individual without the individuals' signed, written authorization. However, a court order may authorize disclosure directly from VHA and the subsequent use of such records to investigate or prosecute VA personnel.

(3) **Disclosures of 38 U.S.C. § 7332 Information for Non-Criminal Purposes.** ***NOTE:*** *There are different criteria for the disclosure of 38 U.S.C. § 7332-protected information without a special authorization pursuant to a special court order depending upon whether the release is for a non-criminal (i.e., civil) or a criminal matter.*

(a) A special court order authorizing the disclosure of personally identifiable information related to 38 U.S.C. § 7332 records for purposes other than criminal investigation or prosecution may be applied for by any person having a legally recognized interest in the disclosure which is sought. The application may be filed separately, or as part of a pending civil action in which it appears that the individual information or records are needed to provide evidence. An application must use a fictitious name (e.g., John Doe) to refer to any individual and may not contain, or otherwise disclose, any individual identifying information unless the individual is the applicant or has given written authorization to disclosure or the court has ordered the record of the proceeding sealed from public scrutiny.

(b) The patient and VA must be given adequate notice and an opportunity to file a written response to the application, or to appear in person, for the limited purpose of providing evidence on whether the statutory and regulatory criteria for the issuance of the court order are met.

(c) Any oral argument, review of evidence or hearing on the application must be held in the judge's chambers or in some manner that ensures that patient identifying information is not disclosed to anyone other than a party to the proceeding, the patient or VA, unless the patient requests an open hearing in a manner which meets the written authorization requirements. The proceeding may include an examination by the judge of the patient records.

(d) An order directing disclosure of 38 U.S.C § 7332-protected records may be entered only if the court determines that good cause exists. To make this determination the court must find that other ways of obtaining the information are not available, or would not be effective, and the public interest and need for the disclosure outweigh the potential injury to the patient, the provider-patient relationship and the treatment services.

(e) An order authorizing a disclosure must limit disclosure to those parts of the patient's record which are essential to fulfill the objective of the order, and those persons whose need for the information is the basis for the order. The order must include such other measures as are necessary to limit disclosure for the protection of the patient, the provider-patient relationship and the treatment services (such as sealing from public scrutiny the record of any proceeding for which disclosure of a patient's record has been ordered).

(4) **To Criminally Investigate or Prosecute 38 U.S.C. § 7332 Patients.**

(a) A court order authorizing the disclosure or use of patient records to criminally investigate or prosecute a patient may be applied for by VA or by any person

conducting investigative or prosecutorial activities with respect to the enforcement of criminal laws. The application may be filed separately as part of an application for a compulsory process, or in a pending criminal action. An application must use a fictitious name to refer to any patient and may not contain or otherwise disclose patient identifying information unless the court has ordered the record of the proceeding sealed from public scrutiny.

(b) Unless an order under paragraph 20.f.(4)(c) is sought with an order under this paragraph 20.d., VA must be given adequate notice of an application by a person performing a law enforcement function. In addition, VA must be given an opportunity to appear and be heard for the limited purpose of providing evidence on the statutory and regulatory criteria for the issuance of the court order and be represented by counsel. Any oral argument, review of evidence or hearing on the application must be held in the judge's chambers, or in some other manner which ensures that patient identifying information is not disclosed to anyone other than a party to the proceedings, the patient or VA. The proceeding may include an examination by the judge of the patient records.

(c) A court may authorize the disclosure and use of patient records for the purpose of conducting a criminal investigation, or for the prosecution of a patient, only if the court finds that all of the following criteria are met:

1. The crime involved is extremely serious, such as one which causes or directly threatens loss of life or serious bodily injury, including homicide, rape, kidnapping, armed robbery, assault with a deadly weapon and child abuse and neglect.

2. There is a reasonable likelihood that the records will disclose information of substantial value in the investigation or prosecution.

3. Other ways of obtaining the information are not available or would not be effective.

4. The potential injury to the patient, to the provider-patient relationship and to the ability of VA to provide services to other patients is outweighed by the public interest and the need for the disclosure.

5. If the applicant is a person performing a law enforcement function, VA has been represented by counsel independent of the applicant.

(d) Any order authorizing a disclosure, or use, of patients' records must limit disclosure and use to those parts of the patient's record which are essential to fulfill the objective of the order and to those law enforcement and prosecutorial officials who are responsible for, or are conducting, the investigation or prosecution. The order must limit their use of the records to the investigation and prosecution of the crime, or suspected crime, that is specified in the application. The order must include any other measures that are necessary to limit disclosure and the use of information to only to the amount of information found by the court to be needed in the public interest.

(5) **Disclosure of 38 U.S.C. § 7332 Information to Investigate or Prosecute VA.**

(a) An order authorizing the disclosure or use of patient records to criminally or administratively investigate or prosecute VA, or employees or agents of VA, may be applied for by an administrative, regulatory, supervisory, investigative, law enforcement or prosecutorial agency that has jurisdiction over VA activities. The application may be filed separately or as part of a pending civil or criminal action against VA (or agents or employees) in which it appears that the records are needed to provide material evidence. The application must use a fictitious name to refer to any patient and may not contain or otherwise disclose any patient identifying information unless the court has ordered the record of the proceeding sealed from public scrutiny or the patient has given a written authorization to the disclosure.

(b) An application may, at the discretion of the court, be granted without notice. Although no express notice is required to VA, or to any patient whose records are to be disclosed, upon implementation of an order that is granted, VA or the patient must be given an opportunity to seek revocation or amendment of the order. This opportunity is limited to the presentation of evidence on the statutory and regulatory criteria for the issuance of the court order.

(c) The order must be entered in accordance with, and comply with, the requirements of non-criminal or criminal purposes. The order must require the deletion of patient identifying information from any documents that are made available to the public.

(d) No information obtained as a result of the order may be used to conduct any investigation or prosecution of a patient or be used as the basis for an application for an order to criminally investigate or prosecute a patient.

g. **Notification to Individual of Disclosures Under Compulsory Legal Process.**

(1) When information is disclosed from an individual's record in response to a court order, and the issuance of that court order is made public by the court that issued it, reasonable efforts must be made to notify the individual of the disclosure.

(2) At the time an order for the disclosure of a record is served at a VA health care facility, efforts must be made to determine whether the issuance of the order has already been made a matter of public record. If the order has not been made a matter of public record, a request must be made to the court by Chief Counsel that the facility be notified when it becomes public.

(3) Notification of the disclosure must be accomplished by informing the individual to whom the record pertains, by mail, at the last known address. The letter must be filed in the record if returned as undeliverable by the U.S. Postal Service.

h. **Use of Undercover Agents and Informants in a 38 U.S.C. § 7332 Program.**

(1) An order authorizing the placement of an undercover agent or informant in a VA drug or alcohol abuse, HIV infection or sickle cell anemia treatment program as an employee or patient may be applied for by any law enforcement or prosecutorial agency

that has reason to believe that employees, or agents of the VA treatment program, are engaged in criminal misconduct. The VA medical facility Director must be given adequate notice of the application and an opportunity to appear and be heard (for the limited purpose of providing evidence on the statutory and regulatory criteria for the issuance of the order). The order may be granted without notice if the application asserts a belief that the Director is involved in the criminal activities or will intentionally or unintentionally disclose the proposed placement to the employees or agents who are suspected of the activities.

(2) An order may be entered only if the court determines that good cause exists. To make this determination the court must find: that there is reason to believe that an employee or agent of VA is engaged in criminal activity; that other ways of obtaining evidence of this criminal activity are not available or would not be effective; and that the public interest and need for the placement of an agent or informant outweigh the potential injury to patients of the program, provider-patient relationships and the treatment services.

(3) The order must specifically authorize the placement of an agent or informant and limit the total period of the placement to 6 months. The order must prohibit the agent or informant from disclosing any patient identifying information obtained from the placement, except as necessary to criminally investigate or prosecute employees or agents of the treatment program. The order must also include any other measures that are appropriate to limit:

(a) Any potential disruption of the program by the placement, and

(b) Any potential for a real or apparent breach of patient confidentiality, such as sealing from public scrutiny the record of any proceeding for which disclosure of a patient's record has been ordered.

(4) No information obtained by an undercover agent or informant may be used to criminally investigate or prosecute any patient or as the basis for an application for an order to criminally investigate or prosecute a patient.

i. **Leave, Fees and Expenses Related to Court Appearances.** The policies concerning court leave, employees appearing as witnesses, temporary duty travel of employees appearing as witnesses and the charging of fees related to such appearances must be addressed with the employees' local payroll office once the local Office of Chief Counsel in the District determines that the employee is required to attend.

j. **Competency Hearings.**

(1) VHA may disclose individually identifiable health information, excluding 38 U.S.C. § 7332-protected information, to private attorneys representing Veterans or VA patients who have been ruled incompetent or declared incapacitated for a competency hearing when a subpoena, discovery request or other lawful process is provided, as long as the Veteran or VA patient has been given notice of the request. There is no authority to

disclose individually identifiable health information to family members or a family member's attorney for the sole purpose of obtaining guardianship. ***NOTE:*** *Authority under both the Privacy Act and HIPAA Privacy Rule is required. Privacy Act routine uses are not adequate authority for disclosure under the HIPAA Privacy Rule. A subpoena does not provide disclosure authority under the Privacy Act. The Privacy Act authority for this disclosure is Routine Use number 8 under the System of Records 24VA10A7, Patient Medical Records-VA. A subpoena does provide disclosure authority under the HIPAA Privacy Rule.*

(2) VHA may disclose individually identifiable health information, excluding 38 U.S.C. § 7332-protected information, to a court, magistrate or administrative tribunal in the course of presenting evidence in matters of guardianship in response to a subpoena, discovery request or other lawful process, when satisfactory assurance in accordance with 45 C.F.R. § 164.512 (e)(1)(ii) has been received.

(3) VHA may disclose individually identifiable information for competency hearings pursuant to a court order without providing the individual a notice.

(4) The individual whose competency is in question cannot authorize disclosure of their own information to a third party or family member for the purposes of a competency hearing. ***NOTE:*** *There is no authority to disclose individually identifiable health information directly to the individual's next-of-kin for a competency hearing unless the next-of-kin is a personal representative (e.g., POA) of the individual.*

k. **Litigation Holds.** When a litigation hold is received from OGC, VA health care facilities are required to maintain and preserve the information and data potentially relevant to the investigation until the litigation hold is lifted. Facility Privacy Officers must work with their Records Officer to ascertain what local facility information is available and any information that may be maintained by a local Business Associate. The VHA Privacy Office is responsible for notifying all national Business Associates. Check with Chief Counsel for any applicable local or VISN litigation holds.

21. LAW ENFORCEMENT ENTITIES

This paragraph covers disclosures to Federal, State, county, local or tribal law enforcement entities, agencies, authorities or officials. An accounting of disclosure is required for any disclosure to any non-VA law enforcement entity.

a. **Parole Office.**

(1) With the signed, written authorization of the patient, personally identifiable information may be disclosed to persons within the criminal justice system if participation in a treatment program is a condition of the disposition of any criminal proceedings against the patient, or of the patient's parole or other release from custody. Disclosure may be made only to those individuals within the criminal justice system who have a need for the information in connection with their duty to monitor the patient's progress (e.g., a prosecuting attorney who is withholding charges against the patient, a

court granting pre-trial or post-trial release, probation or parole officers responsible for supervision of the patient).

(2) The written authorization must be valid, meet the content requirements of paragraph 14 and clearly indicate the period during which the authorization remains in effect. The period must be reasonable, considering:

(a) The anticipated length of the treatment,

(b) The type of criminal proceeding involved, the need for the information in connection with the final disposition of that proceeding and when the final disposition will occur, and

(c) Other such factors considered pertinent by the facility, the patient and the person(s) who will receive the disclosure.

(3) The written authorization must state that it is revocable upon the passage of a specified period of time or the occurrence of a specified, ascertainable event. The time or occurrence upon which authorization becomes revocable must be no earlier than the individual's completion of the treatment program and no later than the final disposition of the conditional release or other action in connection with which the authorization was given.

(4) Information disclosed to individuals within the criminal justice system under this paragraph may be re-disclosed and used only to carry out that person's official job duties with regard to the patient's conditional release or other action in connection with which the authorization was given.

b. **Routine Reporting to Law Enforcement Entities Pursuant to Standing Written Request Letters under 38 U.S.C. § 5701(f).**

(1) Individually identifiable information, excluding 38 U.S.C. § 7332-protected information, may be disclosed to officials of any criminal or civil law enforcement governmental agency or any official instrumentality charged under applicable law with the protection of public health or safety in response to standing written request letters. These law enforcement agencies are charged with the protection of public safety and the implementation of reporting laws of a State which seek reports on the identities of individuals whom VA has treated or evaluated for certain illnesses, injuries, or conditions. While the HIPAA Privacy Rule does not require a written request under 45 C.F.R. § 164.512(f)(1)(i) for reporting mandated or required by law, the Privacy Act and 38 U.S.C. § 5701(f) do.

(2) If the disclosure for routine reporting or a specific law enforcement activity is to a Federal law enforcement entity, that uses 38 U.S.C. § 5701(b)(3) to authorize the disclosure in lieu of 38 U.S.C. § 5701(f); therefore, standing written request letter requirements do not apply.

(3) Information disclosed in response to a standing written request letter is provided for the purpose of cooperating with law enforcement reporting as required by State law. Law enforcement entities routinely require reporting from VHA records for gunshot wounds and other administration action (e.g., suspension or revocation of a driver's license per State mandate). VHA is voluntarily disclosing individually identifiable health information for the purpose of complying with the mandatory reporting as required by State law.

(4) A qualified representative of the agency must make a written request which states the entity is charged with public health and safety (may be inferred based on the agency making the request), the information is requested, the specific law enforcement purpose for which the information is needed, penalties for disclosing information under 38 U.S.C. § 5701(f)(2), the law which authorizes the law enforcement activity or mandated reporting for which records are sought, and signed by a qualified representative of the agency. All requirements in this section of the directive must be met for the Standing Written Request Letter to be valid.

(5) When disclosure of information is made under the provisions of this paragraph the requester must be made aware of the penalty provisions of 38 U.S.C. § 5701(f). If the requester does not indicate awareness of this penalty provision in the request, disclosure of health information must be accompanied by a precautionary written statement worded similarly to the following:

"This information is being provided to you in response to your request (each VA health care facility needs to appropriately identify the request). Please be advised that under the provisions of Title 38, United States Code, section 5701(f), if you willfully use the patient's name or address for any purpose other than for the purpose specified in your request, you may be found guilty of a misdemeanor and fined not more than $5,000 in the case of a first offense and not more than $20,000 in the case of any subsequent offense."

(6) VA health care facilities use the standing written request letter template when soliciting the standing written request letter, by doing so the acknowledgement letter is not required to be sent to the requestor as the template letter has the penalty language included. The standing written request letter must be reissued in writing every 3 years.

(7) If the facility receives an unsolicited standing written request letter and it does not meet the requirements of the template letter then depending on the facility (e.g., VA medical facility, VISN or VHA program office) either the VA medical facility Director or designee or Facility Privacy Officer must acknowledge the receipt of an agency's standing request letter, advise the agency of the penalties using the language in the preceding paragraph regarding the misuse of the information and state that the request letter must be reissued in writing every 3 years.

(8) A file must be maintained for all standing written request letters submitted for information under the provisions of this paragraph. The Facility Privacy Officer must work with VA Police Service to ensure that standing written request letters for law

enforcement agencies are created and maintained as appropriate, with both parties keeping a copy of the current letter on file.

(9) Prior to disclosure of the requested information the assistance of the Chief Counsel may be sought, when appropriate, in evaluating the applicable law relative to the statutory authority of a government agency to gather information on individuals.

(10) An accounting of disclosures must be maintained for all disclosures, including those made to law enforcement authorities, pursuant to a standing written request letter (see paragraph 37.k.).

(11) The standing written request letter authority under 38 U.S.C. § 5701(f) along with the corresponding published standard routine use in VA's Privacy Act Systems of Records are only for routine reporting purposes. Privacy Act, 5 U.S.C. § 552a(b)(7) letters are used for a specific law enforcement activity as opposed to ongoing routine reporting.

c. **Specific Criminal Activity.**

(1) VHA may disclose individually identifiable information, excluding 38 U.S.C. § 7332-protected information, in response to a request received from a law enforcement agency (e.g., Federal Bureau of Investigation, local police department) when such a request is for information needed in the pursuit of a focused (individual specific or incident specific) activity such as a civil or criminal law enforcement investigation authorized by law. The disclosure may be pursuant to 5 U.S.C. § 552a(b)(7), 38 U.S.C. § 5701(b)(3) or (f) and 45 C.F.R. § 164.512(f)(2) depending on information requested. To comply the request must:

(a) Be in writing,

(b) Specify the particular portion of the record desired,

(c) Specify the law enforcement activity or purpose for which the record is sought,

(d) State that de-identified data could not reasonably be used when requesting health information, and

(e) Be signed by the head of the agency.

1. A written request may be signed by an official other than the head of the agency provided that individual has been specifically delegated authority to make requests for information under the authority of 5 U.S.C. § 552a(b)(7). A general delegation of authority is not sufficient to authorize an individual to make requests for information under this disclosure authority. Under the Privacy Act, the delegation of authority may not be made below a section chief. The requester must supply a copy of the written delegation of authority or provide a reference to the delegation such as a C.F.R. citation.

2. Questions as to whether a requester qualifies as the "head of an agency" or an appropriate delegate must be referred to the appropriate Chief Counsel for resolution. For example, a local police investigator could not seek records or be considered an appropriate delegate for the Chief of Police; however, a division chief within the police department could be delegated to act for the Chief of Police.

3. Written requests from VA Offices or VA Programs performing law enforcement activities (e.g., VA OIG, VA Police) must be processed in accordance with paragraph 21.i. below.

(2) Generally, a request for all records pertaining to an individual would not qualify for release under this paragraph. A request for records pertaining to an individual or a group of individuals must be specific as to the records sought (e.g., records for certain types of injuries, for certain time periods).

(3) When disclosure of information is made under the provisions of this paragraph, the requester must be aware of the penalty provisions of 38 U.S.C. § 5701(f) and can demonstrate such awareness through a statement in the request. If the requester does not indicate awareness of this penalty provision in the request, disclosure of health information must be accompanied by a precautionary written statement worded similarly to the following:

"This information is being provided to you in response to your request (each VA health care facility needs to appropriately identify the request). Please be advised that under the provisions of Title 38, United States Code, section 5701(f), if you willfully use the patient's name or address for any purpose other than for the purpose specified in your request, you may be found guilty of a misdemeanor and fined not more than $5,000 in the case of a first offense and not more than $20,000 in the case of any subsequent offense."

(4) Prior to disclosure of the requested information, the assistance of the Chief Counsel may be sought, when appropriate, in evaluating the applicable law relative to the statutory authority of a government agency to gather information on individuals.

d. **Identification and Location of Individuals.**

(1) VHA may disclose limited individually identifiable information to a law enforcement agency or official for the purpose of identifying or locating individuals, such as missing persons or fugitive felons, in response to a written request that meets the requirements of preceding paragraph for Specific Criminal Activity. ***NOTE:*** *This information may be provided to VA Police Officers and VA OIG Officials without a written request.*

(2) In response to a request by law enforcement for the purpose of identifying or locating a suspect, fugitive, material witness or missing person, VHA may provide or disclose only the following information:

(a) Name and address.

(b) Date and place of birth.

(c) SSN.

(d) A, B and O blood type and Rhesus (Rh) factor.

(e) Type of injury.

(f) Date and time of treatment.

(g) Date and time of death, if applicable.

(h) Description of physical characteristics.

e. **Identification and Location of Missing Patients for Health and Safety Reasons.**

(1) A missing patient is an incapacitated patient who disappears from the patient care areas on VA property or while under control of VHA, such as during transport.

(2) VHA may disclose upon its own initiative personally identifiable information to local law enforcement in order to locate missing patients. This information includes name, height, weight, hair color, clothing when last seen and a Veteran Health Identification Card (VHIC) photograph or other photograph, if available. Limited additional information may be disclosed where necessary to convey the urgency of the situation or to assist in handling the patient when located.

(3) VHA Directive 2010-052, Management of Wandering and Missing Patients, dated December 3, 2010, establishes the policy to ensure that each VA health care facility has an effective and reliable plan to prevent and effectively manage wandering and missing patient events that place patients at risk for harm.

(4) The VHIC photo is used for the purpose of identifying the patient when presenting for care (a treatment-related purpose). As a means to enhance the effectiveness of search procedures, each facility is required to establish processes to assure the availability of pictures and physical descriptions for all high-risk patients in the event that they go missing or are suspected of being missing.

f. **Breath Analysis and Blood Alcohol Test.**

(1) Requests by law enforcement officers or government officials for the taking of a blood sample from patients at VA medical facilities for analysis to determine the alcohol content must be denied. In these situations, the requester must be advised that VA personnel do not have authority to withdraw blood from a patient, with or without their authorization, for the purpose of releasing it to anyone for determination as to its alcohol content.

(2) If a blood alcohol analysis is conducted for treatment purposes, then these results may be released with the patient's signed, written authorization. Prior to releasing any blood or alcohol information in response to a valid written request from a civil or criminal law enforcement activity that is made under the provisions of preceding paragraph 21.c., VHA must carefully determine whether this information is protected by 38 U.S.C. § 7332 (i.e., testing was done as part of a drug, alcohol, sickle cell anemia or HIV treatment regimen). If so protected, then the provisions of paragraph 14 must be followed.

(3) VA clinical staff have no authority to conduct chemical testing on patients for law enforcement purposes. However, VA clinical staff need not deny access to VA patients to State and local authorities who, in the performance of their lawful duties, seek to conduct blood alcohol or breath analysis tests (or other similar tests) for investigative or law enforcement purposes, unless the conduct of such tests would create a life-threatening situation for the patient. VA clinical staff must not assist State or local law enforcement officials in the performance of police functions that are outside the law enforcement official's authority. In every case where the authority of the law enforcement official is unclear, Chief Counsel must be contacted for guidance.

g. **Serious and Imminent Threat to Individual or the Public.**

(1) VHA may disclose individually identifiable information, excluding health information, to law enforcement agencies (e.g., Federal, State, local or tribal authorities) charged with the protection of the public health for reporting a serious and imminent threat to the health and safety of an individual or the public without a standing written request letter or written request if, upon such disclosure, notification is transmitted to the last known address of the individual to whom the information pertains (see 5 U.S.C. § 552a(b)(8)).

(2) VHA may disclose individually identifiable health information, excluding 38 U.S.C. § 7332-protected information, to law enforcement agencies charged with the protection of the public health for reporting a serious and imminent threat to the health and safety of an individual or the public without a standing written request letter or written request if:

(a) The law enforcement agency is reasonably able to prevent or lessen the threat, and

(b) Notification is transmitted to the last known address of the individual to whom the information pertains.

(3) VHA may disclose personally identifiable information, excluding 38 U.S.C. § 7332-protected information, necessary for a Federal law enforcement agency to identify or apprehend an individual because of a statement by the individual admitting participation in a violent crime that VHA reasonably believes may have caused serious physical harm to the victim. ***NOTE:*** *For assistance with a disclosure to a non-Federal law enforcement agency, contact the VHA Privacy Office.*

(4) VHA may disclose upon its own initiative personally identifiable information to a family member or individual when necessary to prevent or lessen a serious and imminent threat to the health or safety of that individual.

(5) VHA may not make a disclosure to prevent or lessen a serious and imminent threat if the information was learned in the course of treatment to affect the propensity to commit the criminal conduct or through a request by the individual to initiate or to be referred for treatment, counseling or therapy for the criminal conduct (see 45 C.F.R. § 164.512(j)(2)). Examples include:

(a) An individual admits to committing a rape while being treated for aggressive sexual behavior, or

(b) An individual admits to using illegal drugs or to committing a drug related offense while undergoing drug treatment. ***NOTE:*** *For assistance with a disclosure to a non-Federal law enforcement agency, contact the VHA Privacy Office.*

(6) VHA may disclose individually identifiable information, including relevant health information, excluding 38 U.S.C. § 7332-protected information, to welfare agencies, housing resources and utility companies in situations where VHA needs to act quickly to prevent the discontinuation of services that are critical to the health and care of the individual.

h. **Non-VA Law Enforcement Access to VA Facilities, Patients and Employees.**

(1) A law enforcement official acting officially for an agency having local, State or Federal law enforcement jurisdiction may not be denied access to a VA health care facility, patient or employee.

(2) All non-VA law enforcement officials entering the VA health care facility must be directed upon arrival to the Office of the Director, Chief of Police or the Chief of HRMS to formally disclose the purpose of the visit. The Director and members of the facility staff have no legal authority to prevent lawful questioning, arrest or service of process on a patient or employee.

i. **VA Law Enforcement Activities (VA Office of the Inspector General and VA Police).** VHA may disclose personally identifiable information, including health information, to a VA law enforcement authority or official in accordance with the following paragraphs.

(1) **Routine Reporting.** VHA may disclose personally identifiable information pursuant to a standing written request letter (e.g., fugitive felon reporting (see VHA Handbook 1000.02)).

(2) **Specific Criminal Activity.** VHA may disclose personally identifiable information in response to a written request, including an email request, received from a VA office conducting law enforcement activities when such a request is for information needed in pursuit of a specific criminal investigation. The letter must specify the particular portion

of the record desired, specify that the record is sought for a law enforcement activity and state that de-identified data could not reasonably be used.

(3) **Location and Identification of Individuals.** VHA may disclose limited individually identifiable health information to VA offices performing law enforcement activities for the purpose of identifying or locating individuals. The only information that can be provided is name and address, date and place of birth, SSN, blood type and Rh factor, type of injury, date and time of treatment, date and time of death and a description of physical characteristics. VA Police Officers and VA OIG Officials may be provided this information without a written request.

(4) **Crimes on VA Premises.** VHA may disclose personally identifiable information to VA Police when VHA believes the information constitutes evidence of criminal conduct that occurred on VHA grounds.

(5) **Serious and Imminent Threat to Health or Safety.** VHA may disclose individually identifiable health information, including 38 U.S.C. § 7332-protected information, to a VA law enforcement authority or official for reporting a serious and imminent threat to the health and safety of an individual or the public if VHA believes the VA law enforcement authority or official is reasonably able to prevent or lessen the threat. A notification of the disclosure to VA Police or VA OIG to the last known address of the individual whose information is disclosed is not required as the disclosure is authorized under the Privacy Act need to know exception (5 U.S.C. § 552a(b)(1)).

j. **Drug Enforcement Administration.**

(1) For the purpose of inspecting, copying and verifying the correctness of records, reports or other documents required to be kept or made, the Drug Enforcement Administration (DEA) is authorized to enter VHA-controlled premises and to conduct administrative inspections.

(2) Such entries and inspections must be carried out by DEA inspectors designated by the Attorney General. Any such inspector must present to VHA their appropriate credentials and a written request meeting the requirements of 5 U.S.C. § 552a(b)(7) or DEA Form 82, which provides the DEA inspection authority. The DEA Form 82 must have the following components completed:

(a) Name and title of the owner, operator or agent in charge of the controlled premises.

(b) Controlled premises name.

(c) Address of the controlled premises to be inspected.

(d) Date and time of the inspection.

(e) Statement that a Notice of Inspection is given pursuant to section 50 of the Act (21 U.S.C. § 880).

(f) Reproduction of the pertinent parts of section 510 of the Act.

(g) Signature of the Inspector.

(3) DEA investigators may be given individually identifiable health information, excluding 38 U.S.C. § 7332-protected information. An accounting of disclosure is required.

22. MEDICAL CARE REIMBURSEMENT (REVENUE OPERATIONS)

a. **Third-Party Claims (Tortfeasor, Worker's Compensation).** The individual's signature and assignment of claim on VA Form 4763, Power of Attorney and Assignment, constitutes proper authority to release individually identifiable health information, from the health record to the extent required for VA to effect recovery of the costs for medical care provided to patients in cases in which a third party, such as a tortfeasor, worker's compensation fund, automobile accident reparation insurance or perpetrator of a crime of personal violence, may be liable for costs of medical treatment.

b. **Third-Party Insurance Claims.**

(1) VHA may disclose individually identifiable health information, to any third party or Federal agency, including contractors to those third parties, or to a Government-wide third-party insurer responsible for payment of the cost of medical care in order for VA to seek reimbursement for the cost of medical care or to any activities related to payment of medical care costs (audit of payment and claims management processes) without authorization.

(2) **Health Care Effectiveness Data and Information Set.** The Healthcare Effectiveness Data and Information Set (HEDIS) is a group of measures related to quality of care that is reported by most health plans or insurers within the U.S. It is owned by the National Committee for Quality Assurance (NCQA). Health plans normally cite HEDIS or a purpose of quality review when performing retrospective reviews of Medical Care Collection Fund claims. Relevant information may be disclosed to a Quality Review or Peer Review Organization in connection with the audit of claims or HEDIS reviews to determine the quality of care or compliance with professionally accepted claims processing standards. An authorization is not required to disclose information.

(3) **Accounting of Disclosure.** An accounting of all disclosures of information contained in bills generated from the EHR is maintained as part of the billing system. Any other non-verbal disclosure of health information requires an accounting of disclosure within the ROI Plus software or a separate tracking spreadsheet. Consult the VA medical facility Privacy Officer for additional information.

c. **The Civilian Health and Medical Program.** CHAMPVA is the health care program for the spouses and children of disabled or deceased Veterans administered by the Office of Integrated Veteran Care, which is a part of VHA. CHAMPVA functions similar to a health plan reimbursing non-VA providers for medical care and services

provided to qualified spouses and children of disabled or deceased Veterans. Any disclosures of PHI by the CHAMPVA program are for payment purposes. As with all disclosures, an accounting of disclosures is required as outlined in paragraph 37.l.

d. **Disclosures to Debt Collection Agencies.**

(1) VHA may contract for services to collect a debt owed to VHA. Individually identifiable information may be provided to a contracted collection agency without an authorization for this purpose pursuant to a signed BAA.

(2) VHA cannot provide individually identifiable information to a collection agency contracted for such services until there is a debt owed VHA. For example, a facility cannot use these agencies to verify information that was submitted on VA Form 10-10EZ, Instructions For Completing Enrollment Application for Health Benefits, prior to the incurring a cost for care.

23. NEXT-OF-KIN, FAMILY AND OTHERS

a. **General Inquiry.**

(1) Appropriate VHA clinical staff may disclose general information on individuals to the extent necessary and on a need-to-know basis consistent with good medical or ethical practices to the next-of-kin, family member, close friend or other person(s) with whom the individual has a meaningful relationship.

(2) VHA may use or disclose general information to a member of the public regarding the location or condition of the individual and to a member of the clergy regarding religious affiliation without the written authorization of the individual, as long as the individual is included in the facility directory.

b. **Inquiries in Presence of Individual.**

(1) VHA may disclose personally identifiable information, including health information to next-of-kin, caregivers, family members and others identified by the individual to whom the information pertains in the presence of the individual if:

(a) VHA provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection, or

(b) It is reasonably inferred from the circumstances, based on the exercise of the provider's professional judgment, the individual does not object to the disclosure. ***NOTE:*** *When conducting telehealth visits with an individual located in their residence or other non-VA location, the presence of another person cannot be inferred as the individual not objecting to the disclosure. The individual must be asked if they are agreeable with the disclosure.*

(2) VHA employees are encouraged to document the decision to share information in the above situations or when good medical and ethical practices dictate.

c. **Inquiries Outside Presence of the Individual.**

(1) VHA may disclose individually identifiable health information, excluding 38 U.S.C. § 7332-protected information, to next-of-kin, caregivers, family members and others with a significant relationship to the individual to whom the information pertains, without authorization when, in the exercise of the VHA employee's professional judgment, VHA determines the disclosure is in the best interests of the individual. The disclosure must be limited to information directly relevant to the person's involvement with the individual's health care, payment related to the individual's health care or needed for notification purposes. ***NOTE:*** *The individual listed in the next-of-kin field in the EHR is presumed to be involved in the Veteran's care.*

(2) Inquiries may include, but are not limited to, questions or discussions concerning medical care or home-based care, appointment information, picking up medical supplies and filled prescriptions, questions to call centers and providing forms or other information relevant to the care of the individual. Providing a copy of health records to next-of-kin, family members or any other person still requires the written authorization of the individual or their personal representative.

(3) VHA employees are encouraged to document the decision to share information in the above situations or when good medical and ethical practices dictate.

d. **Human Immunodeficiency Virus Status Notification.**

(1) The VA treating health care provider or a professional counselor may disclose information indicating that a patient is infected with HIV if the disclosure is made to the spouse of the patient, or to a person whom the patient has identified as being a sexual partner during the process of professional counseling for testing to determine whether the patient is infected with the virus (see 45 C.F.R. § 164.512(j) and 38 U.S.C. § 7332(f)).

(2) Disclosure under this paragraph may be made only if the VA treating health care provider makes reasonable efforts to counsel and encourage the patient to provide the information to the spouse or sexual partner and reasonably believes:

(a) That the patient will not provide the information, and

(b) That the disclosure is necessary to protect the health of the spouse or sexual partner.

(3) Disclosure may be made by another VA health care provider or clinical staff member if the VA treating health care provider or counselor who counseled the patient about providing the information to the spouse or sexual partner is unavailable due to absence, extended leave or termination of employment.

(4) Before any patient gives authorization to being tested for HIV, as part of pre-test counseling, the patient must be informed fully about this notification provision.

(5) In each case of a patient with a positive HIV test result who has a spouse or who has identified a person as a sexual partner, the VA treating health care provider or professional counselor must document, in the progress notes of the health record, the factors that are considered which led to a decision to make an un-consented disclosure of the HIV infection information to the patient's spouse or sexual partner. Any such disclosure must be fully documented in the progress notes of the patient's health record.

(6) VHA employee occupational health personnel may disclose an identified source patient's HIV-related information to an exposed employee without authorization from the source patient to the extent reasonably necessary to allow the employee to make an informed decision with respect to available therapeutic alternatives but must not record the source in the employee's medical file unless authorization is obtained from that source.

(7) Disclosures to non-VA employees require the signed, written authorization from the individual prior to disclosing their HIV status (e.g., request from an ambulance transport company whose employee was exposed).

e. **Surrogates Using 38 U.S.C. § 7332-Protected Information.**

(1) A VHA clinical staff may disclose 38 U.S.C. § 7332-protected information to a surrogate of a patient who is the subject of such record if:

(a) The patient lacks decision-making capacity, and

(b) The practitioner deems the content of the given record necessary for the surrogate to make an informed decision regarding the patient's treatment (see 45 C.F.R. § 164.512(j), 38 U.S.C. § 7332(b)(2)(F) and 38 C.F.R. § 1.484).

(2) Whether a patient lacks decision-making capacity is a clinical determination made by the patient's VA treating health care provider.

24. NON-VA HEALTH CARE PROVIDERS (HEALTH CARE PROVIDERS, HOSPITALS, NURSING HOMES, MEDICAL DEVICE VENDORS)

a. VHA may disclose individually identifiable health information to a non-VA health care provider for the purposes of VA paying for services provided by the non-VA health care provider.

b. VHA may disclose any individually identifiable health information, including 38 U.S.C § 7332 protected information, to a non-VA health care provider for the treatment of VA patients. A signed, written authorization of the individual is not required.

(1) Disclosures of individually identifiable health information for treatment of VA patients made verbally do not require an accounting of disclosures.

(2) Disclosures initiated by VA personnel do not require any written request from the non-VA health care provider but require accounting of disclosures.

(3) Requests from non-VA health care providers for a copy of individually identifiable health information require the non-VA health care provider to submit a written request as outlined in paragraph 14.i. and for accounting of disclosure purposes.

c. VHA may disclose individually identifiable health information to resident care homes, nursing homes, assisted living facilities and home health services for the purposes of treatment.

d. VHA may disclose individually identifiable health information to non-VA health care providers through Health Information Exchange (HIE) Partners for treatment of patients. All Veterans are automatically enrolled in Veterans HIE (VHIE) for the sharing of their health information with non-VA health care providers through HIE Partners for treatment of the Veteran. Veterans may opt-out of sharing by submitting VA Form 10-10164, Opt-Out of Sharing Protected Health Information Through Health Information Exchanges, at any time. Details on VHIE are available online at www.va.gov/VHIE.

25. ORGAN PROCUREMENT ORGANIZATION

a. VHA may disclose relevant individually identifiable health information, including 38 U.S.C. § 7332-protected information and the name and address of the patient, to the local Organ Procurement Organization (OPO) or other entity designated by OPO for the purpose of determining potential suitability of a patient's organs or tissues for organ donation without prior signed, written authorization of the patient or personal representative, if the following requirements are met:

(1) The individual must currently be an inpatient in a VA health care facility.

(2) The individual is, in the clinical judgment of the individual's primary or VA treating health care provider, near death or deceased.

(3) The VA health care facility has a signed agreement with the procurement organization.

(4) The VA health care facility has confirmed with HHS that it has certified or recertified the OPO as provided in the applicable HHS regulations.

b. Retrospective requests from an OPO do not meet the intent for determining suitability based on the above four requirements above. If an OPO makes a written FOIA request and provides the names of the deceased Veterans, health information may be released under 38 U.S.C. § 5701 without the personal representative's authorization. This excludes 38 U.S.C. § 7332-protected information, which will be withheld under Exemption 3 of FOIA.

c. An accounting of disclosure is required when disclosing records to an OPO. Verbal conversation with the OPO where information is shared do not require an accounting though documenting such discussions in the health record may be prudent. OPO is considered a health care provider, not a Business Associate of VHA.

d. For additional guidance, contact the VA medical facility OPO coordinator (see 38 C.F.R. § 1.485a).

26. OTHER ENTITIES AND GOVERNMENT AGENCIES

a. **American Red Cross.** VHA may disclose the nature of the patient's illness, probable prognosis, estimated life expectancy and need for the presence of the related active duty Service member to the American Red Cross, for the purpose of justifying emergency leave of the active duty Service member. Information protected by 38 U.S.C. § 7332 may not be disclosed for this purpose.

b. **Bureau of Census.** VHA may disclose personally identifiable information, excluding 38 U.S.C. § 7332-protected information, to the Bureau of Census for purposes of planning or carrying out a census or survey or related activity (see 45 C.F.R. § 164.512(a) and 5 U.S.C. § 552a(b)(4)). If the patient currently admitted to a VA medical facility has opted out of the facility directory, then individually identifiable health information related to the patient's presence in the VA medical facility cannot be disclosed to the Bureau of Census.

c. **Department of Defense.**

(1) **Military Command Authority.** The Military Command Authority allows for appropriate uses and disclosures of PHI concerning members of the Armed Forces to assure the proper execution of the military mission in determining the member's fitness to perform any particular mission, assignment, order or duty. This includes compliance with any actions required as a precondition to performance of such mission, assignment, order or duty.

(a) Military Command legal authority exists for VHA to make the disclosure of a patient's PHI to the military commanding officer without an authorization if:

1. The patient is a member of the Armed Forces,

2. The requester is a military command authority, and

3. The purpose for which the health information is requested is required to meet the military mission.

(b) Relevant health care information may be disclosed to DoD or its components for individuals treated under 38 U.S.C. § 8111A for the purposes deemed necessary by appropriate military command authorities to assure proper execution of the military mission.

(c) Under 10 U.S.C. Part II which governs the Armed Forces, DoD has informally advised that Armed Forces personnel includes all members of the military, active and reserve components, regardless of their duty status at any particular point in time.

(d) Members of the National Guard have two statuses. They are members of the Armed Forces, which is their Federal status. They are also members of the organized State militia, which is not a Federal status. In their Federal status, they are "Armed Forces personnel" for purposes of application of this paragraph on military command authority.

(e) Appropriate military command authority is defined by DoD as all Commanders who exercise authority over an individual who is a member of the Armed Forces, or other person designated by such a Commander to receive PHI in order to carry out an activity under the authority of the Commander. See DoD Manual 6025.18-R 4.4.k.(1)(b)1.

(2) VHA may disclose 38 U.S.C. § 7332-protected information to DoD (TRICARE) without written authorization from active duty personnel for treatment, payment or health care operation purposes.

(3) In general, VHA may disclose personally identifiable information, including 38 U.S.C. § 7332-protected information, on all Veterans and active duty personnel seen at VA without written authorization from the individual for any DoD official purpose. The VA and DoD MOU on Data Sharing outlines the legal authorities for the Departments to share PHI under the HIPAA Privacy Rule.

d. **Other Federal Agencies.**

(1) VHA may disclose personally identifiable information, excluding health information, to another Federal agency if the information is needed in order to perform a function of the requesting agency and if one or more of the disclosure provisions of the Privacy Act, when it applies, permits the disclosure (e.g., routine use disclosure statement under an applicable VHA System of Records).

(2) For reporting to the National Practitioner Data Bank (NPDB), refer to VHA Handbook 1100.17, National Practitioner Data Bank (NPDB) Reports, dated December 28, 2009, and 38 C.F.R. part 46.

(3) For reporting to National Archives and Records Administration (NARA), refer to VA Handbook 6300.1, Records Management Procedures, dated March 24, 2010, and 5 U.S.C. § 552a(b)(6).

(4) For public health reporting to the Centers for Disease Control and Prevention (CDC) or the Food and Drug Administration (FDA), see paragraph 27.

(5) VHA may disclose individually identifiable health information, excluding 38 U.S.C. § 7332-protected information, relating to Veteran health care benefits to another Federal agency that is a HIPAA covered entity who serves Veterans or active duty Service members when the disclosure is necessary to coordinate the functions of the programs or to improve administration and management relating to the programs, and there is a written agreement, such as an MOU, with the Federal agency covering the activity. Contact the VHA Privacy Office for further guidance.

(6) VHA may disclose individually identifiable health information to another Federal agency for other purposes when legal authority exists to make the disclosures under all applicable Federal laws and regulations (e.g., HIPAA, Privacy Act and 38 U.S.C. §§ 5701, 5705 and 7332). Contact the Facility Privacy Officer to determine appropriate legal authority for the disclosure.

e. **National Security.** VHA may disclose personally identifiable information, excluding 38 U.S.C. § 7332-protected information, to authorized Federal officials for the conduct of lawful intelligence or counterintelligence, the protective services of the President or other national security activities:

(1) On its own initiative, when VHA becomes aware of a national security issue, or

(2) Pursuant to a written request letter meeting the requirements under Specific Criminal Activity outlined in paragraph 21.c.

f. **United States Office of Special Counsel.**

(1) OSC is an independent Federal agency that enforces whistleblower protections, safeguards the merit system and provides a secure channel for whistleblower disclosures.

(2) OSC may accept whistleblower disclosures and require VA to investigate these disclosures.

(3) VHA may disclose personally identifiable information to investigators who have been tasked to investigate the whistleblower complaint.

(4) VHA may disclose personally identifiable information, including health information, to OSC in the VA report of findings pursuant to the OSC request letter, which meets the requirements of a Privacy Act, 5 U.S.C. § 552a(b)(7) letter.

g. **Federal Parent Locator Service.**

(1) HHS operates the Federal Parent Locator Service that was established to obtain and transmit information regarding the whereabouts of any absent parent to authorized State agencies to locate such a person for the purpose of enforcing child support obligations.

(2) Individual State parent locator agencies should not contact VA health care facilities directly for address information on absent parents. Any requests received by VA health care facilities for assistance in locating an absent parent must be returned to the requesting agency and the requester must be directed to contact the Federal Parent Locator Service at:

Director, Parent Locator Service Division
Office of Child Support Enforcement
Department of Health and Human Services

370 L'Enfant Promenade SW, Fourth Floor
Washington, DC 20447

27. PUBLIC HEALTH AUTHORITIES

NOTE: *Public health reporting to State Registries, such as* a *State Prescription Drug Monitoring Program or State Immunization Information System, is addressed in paragraph 28.*

a. **Food and Drug Administration.**

(1) **Routine Reporting.**

(a) VHA may disclose individually identifiable health information to FDA or a person subject to the jurisdiction of FDA, (e.g., study monitors) with respect to an FDA-regulated product for purposes of activities related to the quality, safety or effectiveness of such FDA-regulated product. Such purposes include:

1. To report adverse events, product defects or problems or biological product deviations if the person is required to report such information to FDA,

2. To track products if the person is required to track the product by FDA,

3. To conduct post-marketing surveillance to comply with requirements of FDA, or

4. To enable product recalls, repairs or replacement.

(b) A written authorization from the individual is not required if the product in question is FDA-regulated. If not, a signed, written authorization or other legal authority (e.g., waiver of HIPAA authorization) from the individual would be required.

(c) VHA can disclose information covered by 38 U.S.C. § 7332 to FDA when related to treatment with an FDA-regulated product or when part of a research study and the requirements of 38 CFR § 1.488 are met.

(2) **FDA Audit.**

(a) Upon their official written request, authorized FDA agents and investigators are permitted access to individually identifiable health information, including 38 U.S.C. § 7332-protected information, in order to carry out their program oversight duties under the Federal Food, Drug and Cosmetic Act. However, in the event these activities shift from audit to investigation, VHA may disclose personally identifiable information covered by 38 U.S.C. § 7332 only if FDA obtains a court order. If copies of individually identifiable health information are to be provided, the written request must contain agreement to:

1. Maintain the patient identifying information in accordance with the security requirements provided in 38 C.F.R. § 1.466 or more stringent requirements,

2. Destroy all the patient identifying information upon completion of the audit or evaluation, if possible, and

3. Comply with the limitations on disclosure indicating information may be used only to carry out an audit or evaluation purpose or as required by law.

(b) FDA agents may be provided with individuals' names and addresses for the sole purpose of auditing or verifying records. FDA agents must exercise all reasonable precautions to avoid inadvertent disclosure of patient identities to third parties and may not identify, directly or indirectly, any individual patient in any report of such audit or evaluation, or otherwise disclose patient identities in any manner. See 38 U.S.C. § 7332(b)(2)(B) and 38 C.F.R. § 1.489.

(3) An accounting of disclosures in compliance with paragraph 37.k. is required when making a disclosure to FDA.

b. **Routine Reporting to State or Local Public Health Authorities.**

(1) VHA may report a patient's individually identifiable health information, excluding 38 U.S.C. § 7332-protected information, to State or local public health authorities for public health purposes when there is a valid signed standing written request letter between the VA health care facility and the State or local agency that covers the public health reporting of a specific infectious disease or other information, such as vaccinations or vital statistics. For purpose of this reporting, 'patient' means anyone to whom VHA provides a vaccine or care and documents the care in a health record system.

(2) VA, as a Federal agency, is not required to report any patient information to a State for public health reporting even when mandated by State law. Under the Supremacy Clause of the U.S. Constitution, a State cannot compel a branch of the Federal Government to comply with a State mandate that conflicts with a Federal statute. However, in VHA Directive 1131(5), Management of Infectious Disease and Infection Prevention and Control Programs, dated November 7, 2017, the Under Secretary for Health requires VA medical facilities to report infectious diseases to State or local public health authorities when legally permissible.

(3) For a standing written request letter from the State or local public health authority to provide disclosure authority under 38 U.S.C. § 5701(f) and the associated Routine Use Disclosure Statements in VHA Privacy Act Systems of Records notices, VHA may not accept the request unless it:

(a) Be in writing,

(b) State that the agency is charged under applicable law with the protection of the public health or safety and cite the applicable law, if there is any question of such charge,

(c) Specify the public health reporting required and the State law mandating such reporting to the State or local public health authority,

(d) Be signed by a qualified representative of the State or local public health authority requesting the information, and

(e) Be less than 3 years old. A standing written request letter must be submitted by the State or local public health authority and reissued every 3 years.

(4) When disclosure of information is made under the provisions of this paragraph, the requester must be aware of the penalty provisions of 38 U.S.C. § 5701(f). The requester can demonstrate such awareness through a statement in the request. If the requester does not indicate awareness of this penalty provision in the request, disclosure of medical information by VHA must be accompanied by a precautionary written statement worded similarly to the following:

"This information is being provided to you in response to your request for (each VA health care facility needs to appropriately identify the request). Please be advised that under the provisions of Title 38, United States Code, Section 5701(f), if you willfully use the patient's name or address for any purpose other than for the purpose specified in your request, you may be found guilty of a misdemeanor and fined not more than $5,000 in the case of a first offense and not more than $20,000 in the case of any subsequent offense."

(5) An accounting of disclosures in compliance with paragraph 37.k. is required.

c. **Human Immunodeficiency Virus Reporting.**

(1) Information relating to an individual's infection with HIV may be disclosed to a Federal, State or local public health authority that is charged under Federal or State law with the protection of the public health, and to which Federal or State law requires disclosure of such record, if a qualified representative of such authority has made a written request that such record be provided as required pursuant to such law for a purpose authorized by such law. In the case of a State law, such law must, in order for VA to be able to release patient name and address information in accordance with 38 U.S.C. § 5701(f)(2), provide for a penalty or fine or other sanction to be assessed against those individuals who are subject to the jurisdiction of the public health authority but fail to comply with the reporting requirements. See 38 C.F.R. § 1.486.

(2) A State public health authority to whom a record is disclosed under this section may not redisclose or use such record for a purpose other than that for which the disclosure was made.

(3) An accounting of disclosures in compliance with paragraph 37.k. is required.

d. **Influenza (Flu) Vaccination.**

(1) If a VA health care facility has a standing written request letter that meets the requirements of paragraph 27.b.(3) with the public health department that covers influenza illness and vaccination, the facility may choose to provide vaccination information or influenza illness information if it is determined that it is in the best interests of the facility, community or State. An accounting of disclosures in compliance with paragraph 37.k. is required.

(2) In the interests of collaboration with states and in order to provide the best data to the CDC, the VHA National Center for Health Promotion and Disease Prevention encourages reporting of de-identified, aggregate data to States, such as number of vaccinations given by age or risk group. Reporting of de-identified data does not require a signed standing written request letter.

(3) While influenza (flu) vaccination is a mandatory condition of employment for VHA health care personnel, EOH cannot send a list of employees who have not or have received the flu vaccination to supervisors, HR or facility leadership. EOH may provide vaccination rates to facility departments, as long as, the group is large enough that individuals cannot be identified. EOH may identify to VA health care facility executive leadership those personnel who have not signed and submitted the VA Form 10-9050, HCP Influenza Vaccination Form, as outlined in VHA Directive 1192.01, Seasonal Influenza Vaccination Program for VHA Health Care Personnel, dated August 10, 2020.

e. **Centers for Disease Control and Prevention.**

(1) VHA may report individually identifiable health information, excluding 38 U.S.C. § 7332-protected information, for public health activities and purposes to CDC as a public health authority that is authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury or disability. Public health activities include, but are not limited to, the reporting of disease or the conduct of public health surveillance, including immunization reporting, public health investigations and public health interventions.

(2) Names and addresses of Veterans or their beneficiaries are provided to CDC under 38 U.S.C. § 5701(b)(3). ***NOTE:*** *If information is provided to CDC from a VHA Privacy Act System of Records other than 24VA10A7, Patient Medical Records-VA, or 172VA10A7, Corporate Data Warehouses-VA, the VHA Privacy Office must be contacted for guidance.*

f. **Public Health Crisis.** Disclosures may be made to public health authorities when there is a public health crisis resulting in a serious and imminent threat to the health or safety of the public and society, such as with a pandemic, and other public health legal authority for the disclosure is not present as outlined below. ***NOTE:*** *Only positive test results of infectious diseases, such as COVID-19, may be released when authorizing disclosure using the serious and imminent threat justification.*

(1) VHA may disclose individually identifiable information, excluding 38 U.S.C. § 7332-protected information, to Federal, State and local public health authorities

pursuant to a written request from the entity referencing a declared state of emergency in the jurisdiction due to the public health crisis. See 38 U.S.C. § 5701(e) and 5 U.S.C. § 552a(b)(8).

(2) Any disclosure of individually identifiable information under the serious threat to health or safety provision of the Privacy Act, 5 U.S.C. § 552a(b)(8) requires written notification to the last known address of the individual to whom the information pertains. If other Privacy Act authority is applied (e.g., Routine Use in applicable System of Records notice), such notification is not required.

28. REGISTRIES

a. **Private Registries.** VHA may not disclose individually identifiable information to private registries without the prior signed, written authorization of the individual to whom the information pertains.

b. **State Cancer Registries.** VHA may disclose individually identifiable health information, excluding 38 U.S.C. § 7332-protected information, to any State cancer registry upon the written request of the State when required by State law. The written request may be considered standing for ongoing reporting to the State cancer registry if continuous reporting is requested and the requirements of a standing written request letter as outlined in paragraph 27.b.(3) are met. A standing written request letter is valid for 3 years, at which time it must be reissued. An accounting of disclosure is required. See VHA Directive 1412(1), Department of Veterans Affairs Cancer Registry System, dated May 29, 2019.

c. **State Prescription Drug Monitoring Programs.**

(1) VHA may disclose individually identifiable health information, including 38 U.S.C. § 7332-protected information, to a State Prescription Drug Monitoring Program (PDMP) without the signed, written authorization of the patient for whom the medication was prescribed. Disclosure may be for the purpose of querying the PDMP or reporting mandatory prescription information to the State (e.g., batch reporting).

(2) VA medical facility Privacy Officers must work with their clinical staff to ensure that an accounting of disclosures is created when querying the PDMP. Querying the PDMP directly through the electronic health record automatically creates an accounting of disclosure.

(3) A computer route has been created to automatically capture the accounting of disclosures elements for batch or system reporting made through the EHR. VHA employees do not have to take any action to account for such disclosures.

(4) **Reporting to Other Public Registries.** VHA may disclose individually identifiable health information, excluding 38 U.S.C. § 7332-protected information, to any other public registry (e.g., Federal, State, local or tribal), such as a State Immunization Information System, for reporting purposes upon written request when required by law and the request meets the requirements of 38 U.S.C. § 5701(f).

d. **Querying Other State or Public Registries.**

(1) A VA treating health care provider or other clinical staff may query other State registries for the purpose of obtaining or verifying health information, such as vaccinations, for treatment of the Veteran or patient without obtaining a signed, written authorization from the Veteran or patient. Veteran or patient names and other identifiers may be disclosed to the State registry to query the registry for treatment purposes as legal authority under all applicable Federal privacy laws and regulations exists. Legal authority to disclose individually identifiable health information does not negate any policy requirements from VHA programs, such as obtaining agreements with the State registry, that must be adhered to prior to querying the registry.

(2) An accounting of disclosures is not required for a querying a State registry if:

(a) The only information shared with the State registry as part of the query are the name or other identifier of the patient, such as date of birth, and either

(b) The State or other public registry does not retain any of the information used to look up the Veteran or patient, such as name and date of birth, in the registry, or

(c) The State or other public registry is only retaining a transactional log of the information used to look up the Veteran or patient in the registry for cybersecurity purposes.

(3) The VHA Privacy Office must be contacted to determine if an accounting of disclosures in compliance with paragraph 37.k. must be maintained for the specific query.

29. STATE VETERANS HOMES

a. State Veterans Homes are established by a State to provide nursing home, domiciliary or adult day health care for eligible Veterans. State Veterans Homes are owned, operated, managed and financed by States. VA provides Federal assistance to States by participating in a percentage of the cost of construction and paying per diem. VA assures the Secretary, Congress and Veterans that State Veterans Homes meet VA standards through annual surveys, audits and reconciliation of records. VA does not have the authority to manage or intervene in the management of the facility's operations.

b. VHA may disclose a Veteran's individually identifiable health information, including 38 U.S.C. § 7332-protected information, to a State Veterans Home for treatment or follow-up at the State Veterans Home, whether or not VA is paying a per diem rate to the State Veterans Home for the resident receiving care at such Home as the disclosure is for treatment.

c. State Veterans Home access to the EHR of a patient will be managed at the facility level. CPRS Read Only will be used to limit access of authorized State Veteran Home employees' access to a specified claimant's VHA EHR. State Veterans Home

access to CPRS Read Only will be contingent upon each patient executing a request for and authorization to release health information that authorizes the State Veterans Home to have unlimited and unrestricted access to all health records, including records protected by 38 U.S.C. § 7332. The VHA Health Information Access (HIA) office must be contacted for guidance.

30. VETERANS SERVICE ORGANIZATIONS

a. VHA may disclose personally identifiable information, including 38 U.S.C. § 7332-protected information and all other health information to a Veterans Service Organization (VSO) for purposes of obtaining benefits, provided an appropriate legal POA allowing access to the Veteran's health records through the use of VA Form 21-22 or VA Form 21-22a has been filed with VA, either through the VHA HIA office for electronic access via the Compensation and Pension Records Interchange or with VBA directly. If a written request is received from a VSO for individually identifiable health information, VHA must verify through VBA that a POA is on file or obtain a copy of the POA from the VSO representative.

b. The POA must include specific authority in order to disclose 38 U.S.C. § 7332-protected information if VA Form 21-22 or VA Form 21-22a is not used.

c. If the VSO does not have an appropriate POA, disclosure may be made only pursuant to a signed, written authorization from the individual to whom the information pertains.

d. VSOs cannot be provided a copy of a VA medical facility's Gains and Losses sheet because there is no authority to disclose this information. Questions from VSOs on this matter need to be forwarded to the Facility Privacy Officer.

e. VSO employees may be provided with access to a VHA EHR system that limits their access to a specified claimant's health record, contingent upon the claimant executing a POA or an authorization to release health information, authorizing the VSO unrestricted access to all the specified claimant's health records, including records protected by 38 U.S.C. § 7332.

31. COMPENSATED WORK THERAPY

a. VA provides patients with rehabilitative services through a program commonly referred to as the Compensated Work Therapy (CWT) program. Under this program, Veteran patients may work in VA health care facilities providing services as a form of rehabilitative medical treatment.

b. CWT patients are not considered employees for purposes of having access to Veteran patient health records; therefore, they are not required to take privacy or security training. They are not considered volunteers because VA volunteers serve as without-compensation employees.

c. Absent a signed, written authorization from the Veteran, there is no current authority under the Privacy Act, HIPAA Privacy Rule or 38 U.S.C § 7332 to disclose individually identifiable patient health information to CWT patients. CWT patients cannot work in escort/volunteer areas, inpatient wards, outpatient/clinic areas, domiciliary areas or nursing home areas unless the Veteran's authorization is obtained. CWT patients can work in engineering, Acquisitions Material Management, housekeeping, greeting desk/directional desk (no gains and losses sheets) or mail room sorting mail but cannot open the mail or deliver mail to individual Veteran rooms.

32. WORK STUDY STUDENTS AND STUDENT VOLUNTEERS

a. Work study students are considered employees during the time they are enrolled in school and working for VA. A work study program compensates VA for the work that these students perform. Work study students can work in patient care areas as long as they have completed their privacy and security training. Work study students can have access to PHI after they have completed the required privacy training. If they access computer systems, they are required to complete the mandatory security training and complete a background check.

b. Student volunteers under the age of 18, or those who have not reached the age of majority in the State in which they are volunteering for VA, must have written parental or guardian approval to participate in the VA Center for Development and Civic Engagement, and must have written authorization for diagnostic and emergency treatment if injured while volunteering. Student volunteers must not be given electronic access to any individually identifiable information, such as EHR data, in the performance of their voluntary duties. Student volunteers may be given verbal or paper personally identifiable information after the completion of privacy training.

33. DECEASED INDIVIDUALS

a. **General Rule.**

(1) VHA must protect the individually identifiable health information about a deceased individual to the same extent as required for the individually identifiable health information of living individuals, for as long as VHA maintains the health records. ***NOTE:*** *See RCS 10-1 for retention requirements of VHA records.*

(2) Though VHA is only required to comply with guidelines regarding appropriate uses and disclosures of a deceased individual's PHI under the HIPAA Privacy Rule for a period of 50 years following the death of the individual, VHA applies the HIPAA Privacy Rule for as long as VHA maintains the individual's health records. However, unlike the HIPAA Privacy Rule and 38 U.S.C. §§ 5701 and 7332, the Privacy Act does not apply to records of deceased individuals.

b. **Deceased Veterans' Information.**

(1) The personal representative of a deceased individual has the same HIPAA Privacy Rule rights as the deceased individual and may exercise all of the HIPAA

Privacy Rule rights of that individual, including filing an amendment request and signing an authorization for the use and disclosure of the deceased individual's record. ***NOTE:*** *For further information on personal representatives, see paragraph 5.*

(2) VHA must disclose to the personal representative the individually identifiable health information, excluding 38 U.S.C § 7332-protected information, of the deceased individual pursuant to the personal representative's signed written request under the HIPAA Privacy Rule right of access provisions.

(3) VHA may disclose individually identifiable health information, excluding 38 U.S.C § 7332-protected information, about a deceased individual under the following circumstances:

(a) To a law enforcement official for the purpose of alerting law enforcement of an individual's death, if VHA has a suspicion that such a death may have resulted from criminal conduct. A standing written request letter in compliance with 38 U.S.C. § 5701(f) must be on file.

(b) To a coroner or medical examiner for the purpose of identifying a deceased person, or for other duties authorized by law.

(c) To a family member's provider, when it is determined that it is relevant to the treatment of a decedent's family member, or consistent with applicable law.

(d) To funeral directors, as necessary, to carry out their duties with respect to the decedent. VHA may disclose the individually identifiable health information prior to, and in reasonable anticipation of, the individual's death.

(e) To family members of the deceased individual when appropriate authority under FOIA permits (see paragraph 33.d.).

(f) To any other party for whom there is authority under the HIPAA Privacy Rule and 38 U.S.C. § 5701 to make the disclosure.

(4) VHA may use, or disclose, individually identifiable health information, excluding 38 U.S.C. § 7332-protected information, of a decedent for research purposes without authorization by a personal representative, and absent review by an IRB or privacy board, as long as VHA receives the following:

(a) Oral or written representation that the individually identifiable health information sought will be used or disclosed solely for research on decedents,

(b) Documentation of the death of such individual, if requested by VHA, and

(c) Representation from the requester that the individually identifiable health information for which use or disclosure is sought is necessary for the research purposes.

c. **Deceased Veterans Information that Includes 38 U.S.C. § 7332 Information.**

(1) VHA may disclose individually identifiable health information, including 38 U.S.C § 7332-protected information, about a deceased individual when legally authorized by that statute, including, but not limited to, the following circumstances:

(a) To a community care provider for treatment or health care operations. VHA will respond to requests from community care providers through VHIE for only 6 months after the individual's date of death.

(b) To an OPO as outlined in paragraph 25.

(c) To a third party in order to recover or collect reasonable charges for care furnished to, or paid on behalf of, a patient in connection with a non-service-connected disability as outlined in paragraph 22.

(2) Authorization for disclosures from the record of a deceased patient treated for drug or alcohol abuse, HIV or sickle cell anemia may be given by the next-of-kin, executor, administrator or other personal representative only for the purpose of obtaining benefits to which the deceased patient's survivor(s) may be entitled. This would include not only VA benefits, but also payments by SSA, Worker's Compensation Boards or Commissions, other Federal, State or local government agencies or non-government entities, such as life insurance companies, and the pursuit of legal action.

(3) Under the survivorship benefit provision, sickle cell anemia information may be released to a blood relative of a deceased Veteran for medical follow-up or family planning purposes.

(4) Disclosures may be made without written authorization from the deceased individual's personal representative in order to comply with Federal or State laws requiring the collection of death and other vital statistics.

(5) Information may be disclosed to a coroner or medical examiner in response to written request in order to permit inquiry into a death for the purpose of determining cause of death.

(6) Information must only be used within VHA and disclosed outside VHA for research purposes pursuant to the research provisions, see paragraph 13.

d. **Family Members Requesting Deceased Veterans' Records.**

(1) VHA may disclose individually identifiable health information, excluding 38 U.S.C § 7332-protected information, about a deceased individual pursuant to any family member's FOIA request when such disclosure is not an unwarranted invasion of the personal privacy of any surviving family members.

(2) When an individual is deceased, FOIA Exemption 6 no longer applies to the personal privacy of the individual. It applies to protecting the individual's surviving family

members from an unwarranted invasion of personal privacy. The personal representative of the individual is not required to authorize disclosure to a family member under a FOIA request. ***NOTE:*** *FOIA requires disclosure and falls under the HIPAA Privacy Rule Required by Law provision, 45 C.F.R. § 164.512(a). Therefore, only FOIA Exemptions apply in regard to family members obtaining a deceased Veterans' records, and FOIA Exemption 6 cannot be used to protect the privacy of a family member from themselves (e.g., cannot use Exemption 6 to protect the surviving spouse when the spouse is making the FOIA request). Other FOIA Exemptions may apply.*

e. **Autopsy Findings.**

(1) A copy of the autopsy clinical finding summary and the listing of clinical-pathological diagnoses may be disclosed when requested by the personal representative of the individual.

(2) In all cases where the autopsy protocol reveals 38 U.S.C. § 7332-protected information, the autopsy protocol must not be disclosed to the next-of-kin unless the VA medical facility Director determines that such disclosure is necessary for the survivor to receive VA benefits. These records may be released for other than survivorship benefit purposes if those portions relating to the 38 U.S.C. § 7332-protected information can be appropriately deleted under FOIA. Under the survivorship benefit provision, sickle cell anemia information may be released to a blood relative of the deceased Veteran for medical follow-up or family planning purposes.

(3) The autopsy protocols may be released to a private provider when specifically requested in writing by personal representative or the next-of-kin.

(4) If there is any indication that the requested information will be used in a lawsuit, the Chief Counsel must be informed promptly of the circumstances. No further actions can be taken without guidance from the Chief Counsel.

34. VHA SYSTEMS OF RECORDS

a. The VHA Privacy Office manages the Privacy Act System of Records processes for VHA and the VHA program offices who are responsible for the information collected and covered in their System of Records. Each VHA program office that owns information covered by a Privacy Act System of Records must provide a point of contact name and contact information for their SORN. ***NOTE:*** *The VHA Privacy Office cannot be the owner of a VHA or OIT Privacy Act System of Records. The System Manager is the VHA official or program office assigned the responsibility for a Privacy Act-covered System of Records as identified in the system description that is published in the Federal Register in accordance with VA Handbook 6300.5. The VA health care facility official with the program assignment is responsible for the maintenance of the records at the facility.*

b. Information concerning an individual is not collected or maintained in such a manner that the information is retrieved by an individual's name or unique identifier

unless a notice is first published in the Federal Register. Without prior publication of a SORN, such a system would be an illegal System of Records, and the personnel operating it could be exposed to criminal penalties under the Privacy Act. This requirement applies to information about an individual that is maintained in any record or storage medium, including paper records or documents, personal computers, computer systems and local and national databases.

c. Prior to collecting or maintaining information concerning an individual in what would be a Privacy Act System of Records, the VA health care facility must verify the existence of a published SORN. If it is determined that a published SORN does not exist, the VHA Privacy Office must be contacted for assistance prior to any new collection of information or new use of existing information. ***NOTE:*** *Contact the VHA Privacy Office if assistance in this determination is needed.*

d. Prior to collecting information from an individual, the VA health care facility needs to ensure compliance with the Paperwork Reduction Act and 5 C.F.R. part 1320, Controlling Paperwork Burdens on the Public and inclusion of a Privacy Statement.

e. Records are not to be established and information collected until the SORN is approved by the VHA Privacy Office and submitted for approval by the Secretary of Veterans Affairs or designee for publication in the Federal Register for public comment, and appropriate reports are submitted to OMB and Congress.

f. Components of a Privacy Act SORN are outlined in VA Handbook 6300.5 and OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.

g. Records maintained in a VHA System of Records will be used and released in accordance with policies outlined in this directive. Records commonly used within a VA medical facility covered by a VHA SORN are in the Privacy Act System of Records 24VA10A7, Patient Medical Records-VA. For a list of all VHA Systems of Records notices, see: https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/SystemofRecords.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

35. RELEASE FROM NON-VHA SYSTEMS OF RECORDS

a. Within VA health care facilities, several non-VHA Privacy Act Systems of Records are subject not only to the provisions of the Privacy Act but also to VA Confidentiality Statutes. Non-VHA Systems of Records include, but are not limited to, Official Personnel Folders (OPF), Employee Medical Folder, VBA Compensation and Pension File and VA Police Records. While the Employee Medical File Folder is a non-VHA Privacy Act System of Records, when maintained by VHA EOH, as part of the HIPAA covered entity, it is PHI subject to the HIPAA Privacy Rule.

b. If, for example, a VHA employee produces a health record in support of a patient's claim for VA disability benefits, this copy of the health record placed in the VBA Compensation and Pension file is under the authority of the local VBA Regional Office.

If the VA medical facility has VA benefits health information such as Compensation and Pension exams, refer to the VA medical Facility Privacy Officer for disclosure guidance.

c. Questions regarding right of access, amendment or release of non-VHA records/information must be referred to the non-VHA System Manager (e.g., VBA, HRMS) who has responsibility over these records, who will make the determination regarding access, amendment or release based on Federal Privacy and Confidentiality Statutes, VA regulations and official policies of the non-VHA record. The Employee Medical Folder of VHA employees falls under VHA EOH for guidance.

d. VA health care Facility Privacy Officers must work with these offices to determine how to process such requests.

NOTE: *See Appendix B for a list of non-VHA Systems of Records that may be maintained within a VA health care facility.*

36. OTHER TYPES OF USES, DISCLOSURES AND RELEASES

a. **Affiliated Educational Institutions and Accrediting Bodies.**

(1) VHA may disclose individually identifiable health information, excluding 38 U.S.C. § 7332-protected information, to an Affiliated Educational Institution and Accrediting Body for health care operations, providing there is an acknowledgement agreement in place with the receiving institution. This acknowledgement will ensure that, when an Affiliated Educational Institution receives VHA PHI for purposes of educational program administration, quality assurance activities or other assessments, the affiliated educational institution will collect, store and protect this information according to all applicable privacy laws and standards.

(2) Affiliated Educational Institutions and Accrediting Bodies (e.g., American College of Surgeons or the Accreditation Counsel for Graduate Medical Education (ACGME)) need PHI for the following purposes in the administration of educational programs, quality assurance activities and other assessments:

(a) To assess the competency of HPTs and staff.

(b) To assess the number and types of patients from which HPTs learn, or that staff members care for.

(c) To comply with clinical or education accreditation standards.

(d) For academic or disciplinary actions involving HPTs or staff for which individually identifiable health information is relevant.

(e) To assess and improve the quality of care during training and learning activities.

(3) VHA and the respective Affiliated Educational Institution or Accrediting Body are encouraged to exchange de-identified data whenever such data is sufficient and will not require an acknowledgement agreement.

(4) When VHA individually identifiable health information is disclosed to Affiliated Educational Institutions or Accrediting Bodies either directly, through HPTs or faculty members, copies of that data that have been disclosed become the property of the Affiliated Educational Institutions and are no longer considered part of a VHA Privacy Act System of Records. The requirement to account for the disclosure must be followed.

b. **Audit and Evaluation Purposes.**

(1) To the extent that personally identifiable information, including name and address and 38 U.S.C. § 7332-protected information is relevant and necessary to the conduct of an audit or evaluation not addressed by other paragraphs, records may be reviewed by or disclosed to the following:

(a) VA personnel who need the information for audit or evaluation purposes such as: special purpose or site visits, audits and reviews under the Health Systems Review Organization (HSRO) Program, compliance review audits or assessments and clinical and administrative audits.

(b) Evaluation agencies under contract with VA that are charged with facility-wide monitoring of all aspects of patient care (such as The Joint Commission) pursuant to a BAA.

(c) Evaluation agencies under contract with VA that are charged with more narrowly focused monitoring (e.g., College of American Pathologists, American Association of Blood Banks, External Peer Review) to the extent that the information is relevant to their review pursuant to a BAA.

(2) Individuals who conduct an audit or evaluation and receive or review personally identifiable information must be advised that the information is provided or disclosed for audit or evaluation purposes only and that given its private, confidential nature, the information needs to be handled with appropriate sensitivity.

(3) Individuals who conduct an audit or evaluation and receive or review 38 U.S.C. § 7332-protected information must not identify, directly or indirectly, any individual patient or subject in any report of audit or evaluation, or otherwise disclose patient or subject identities in any manner outside of VA.

c. **Auditory Privacy.**

(1) VHA is committed to appropriately safeguarding and ensuring patient confidentiality regarding auditory personally identifiable information in facility operations, including during the check-in process.

(2) Employees must exercise appropriate precautions and safeguards when discussing Veterans' personally identifiable information in open or public areas, such as clinic waiting rooms. Appropriate safeguards for auditory privacy include:

(a) Using VHIC for identification upon check-in, if available.

(b) Using an appropriate volume of voice when speaking with the Veteran in a public area or during check-in.

(c) Requesting or discussing only the information necessary to accomplish the function; for example, not asking for the full SSN when the last four digits will suffice.

(d) Asking other Veterans in line for clinic check-in to wait a sufficient distance away from the desk to allow a zone of audible privacy as opposed to being right behind the Veteran being assisted. If space allows for 10-foot proximity around the waiting room front desk, a sign will be posted (e.g., "Please allow for patient confidentiality by keeping behind this sign until called.").

(e) Discussing personal information of the Veteran only in private areas, such as behind a closed door.

(3) To ensure auditory privacy awareness and implementation of appropriate safeguards, the VA health care facility must place signs alerting Veterans to auditory privacy concerns in the waiting areas, elevators and other spaces requiring auditory privacy.

(4) Chairs in waiting rooms must be placed as far from the reception desk as possible.

(5) Check-in kiosks must have privacy screens and be placed in a manner that individuals in the waiting area or walking past cannot see what personally identifiable information is being entered by the Veteran.

d. **Certification Boards.**

(1) VHA may disclose non-identifiable information as defined in this directive to certification boards under health care operations for the purpose of clinical staff to obtain certification or licensing. Certification boards requiring health information from VA providers and HPTs must not include any unique identifiers before disclosure. Only non-identifiable information, which has the unique identifiers removed, may be provided. A BAA and DUA are not required with the certification board.

(2) VA providers maintaining a listing of Veterans' personally identifiable information for submission of non-identifiable information to their certification boards must safeguard this personally identifiable information on a shared network drive and not on a physical log.

e. **Claims Folder (Veterans Benefit Administration).**

(1) Requests for release of health information in Veterans' claims folders must be referred to the VBA Regional Offices. Copies of compensation and pension (C&P) examinations that are maintained in the patient health record may be released by the VA health care facility in accordance with this directive; however, there is a 20-business-day hold on C&P exams prior to release. ***NOTE:*** *Review the ROI Plus Software User Manual for the process for disclosing C&P exams. For additional information please see VHA Directive 6370, Compensation and Pension (C&P) Examination Report Release of Information, dated August 22, 2019.*

(2) A Hospital Inquiry (HINQ) is a request that is sent to VBA from the VA medical facility for information pertaining to a Veteran. VHA uses the HINQ to upload information directly into the patient file. The information in the HINQ may be disclosed by VHA as the HINQ software is part of the VistA-VA System of Records 79VA10A7, even though the HINQ request is not maintained after the information is placed within the EHR. Any request to amend the information received through a HINQ request must be referred back to VBA.

f. **Credentialing and Privileging Records.**

(1) VHA provider credentialing and privileging records are VHA records and are covered under the VHA Privacy Act System of Records 77VA10E2D, Health care Provider Credentialing and Privileging Records-VA.

(2) Requests for VHA provider credentialing and privileging information or records need to be processed in accordance with VHA Directive 1100.20, Credentialing of Health Care Providers, dated September 15, 2021; VHA Directive 1100.21(1), Privileging, dated March 2, 2023.; the Privacy Act; FOIA and the provisions of this directive as outlined below.

(a) Requests from VHA providers for copies of their own records maintained in the Credentialing and Privileging file as part of the VHA Privacy Act System of Records 77VA10E2D, Health care Provider Credentialing and Privileging Records-VA, will be processed as a first-party right of access request under the Privacy Act.

(b) Requests from third parties for copies of credentialing and privileging information require a signed, written authorization from the VHA provider or other legal authority under the Privacy Act prior to disclosure. If no Privacy Act authority exists and the request was received in writing, the request will be processed under FOIA.

(3) Each privileged health care provider must have a Credentialing and Privileging file established electronically in VetPro or other established IT system, with any paper documents maintained according to the requirements of the standardized folder. Other credentialed clinical staff may have a credential file maintained in the same Privacy Act System of Records even though they may not be granted clinical privileges.

g. **Incidental Disclosures.**

(1) Due to the nature of communications and practices, as well as the various environments in which Veterans receive health care or other services from VHA, the potential exists for a Veteran's health information to be disclosed incidentally pursuant to an otherwise permitted or required use or disclosure. For example:

(a) A hospital visitor may overhear a provider's confidential conversation with another provider or a patient.

(b) A patient may see limited information on clinic sign-in sheets, such as patient names and appointment times, or another patient's full name or last name with first initial on bingo boards or monitors.

(c) A Veteran may hear another Veteran's name being called out for an appointment.

(d) A Veteran may hear a conversation that a provider is having with another patient while waiting to be seen in the ER due to curtains dividing the ER.

(2) Reasonable safeguards to protect the privacy of information from incidental disclosures must be deployed. When reasonable safeguards are deployed to limit incidental disclosure of the information there is no violation of privacy law or regulation. Examples of reasonable safeguards include:

(a) Speaking quietly when discussing a patient's condition with family members in a waiting room or other public area.

(b) Avoiding using patients' names in public hallways and elevators and posting signs to remind employees to protect patient confidentiality.

(c) Paging individuals without identifying them as a patient or linking the individual with an appointment or potential health information.

(d) Using VHIC for identification of the patient.

(e) Limiting the patient information or identifiers displayed on white boards in clinical treatment areas to only the minimum information required for the treatment function.

(3) A lack of training is not a valid excuse for unauthorized disclosures resulting from failure to follow the reasonable safeguards regarding incidental disclosures. Unauthorized disclosures are often a result of negligence, mistakes or failures to follow reasonable safeguards.

(4) Displaying information in an Emergency Department waiting area can include the following data elements: location (room/bed/department); patient's last name (also first name, if last name is not enough to uniquely identify the person); provider/HPT/nurse initials; and elapsed minutes. Other data elements may be included if determined to be clinically relevant and limited to the minimum extent possible after consulting with the VA medical facility Privacy Officer.

(5) Displaying information in treatment areas that are not viewable by the public, the following data elements could be displayed: location (room/bed/department); patient last name; complaint; comment; provider/HPT/nurse initials; acuity (a number from 1-5); number of unverified orders; number of active orders/number of completed orders; and elapsed minutes. The patient's name can be posted outside of the patient's room. Other data elements may be included if determined to be clinically relevant and limited to the minimum extent possible after consulting with the VA medical facility Privacy Officer.

(6) When posting treatment guidelines in a patient's room, the titles must never include specific diagnoses or medical conditions or indicate a specific disorder. A generic title such as Ambulatory Guidelines, Feeding and Swallowing Guidelines or Universal Precautions is acceptable. A guideline such as Alzheimer's Precautions would not appropriately safeguard the patient's information from the public.

h. **Medical Opinions/Forms Completion.**

(1) VA treating health care providers are required, when requested and under certain limited circumstances, to provide descriptive statements and opinions and to fill out medical forms for a VA patient with respect to patient's medical condition, employability and degree of disability (see 38 C.F.R. § 17.38 and VHA Directive 1134(2), Provision of Medical Statements and Completion of Forms by VA Health care Providers, dated November 28, 2016). VA treating health care providers may provide these forms directly to the patient using VA Form 10-5345a. If the patient requests a copy of the note where the form is talked about and the information is part of discharge planning, then VA Form 10-5345a is not required. However, if the VA treating health care provider is asked to provide the form directly to a third party, such as an employer or benefits agency, the VA treating health care provider must either have the patient fill out VA Form 10-5345 or refer them to the ROI Department to ensure appropriate legal authority exists for the disclosure and accounting of disclosure is created.

(2) **Support of VA Benefits Claims.**

(a) An individual may request statements from VA treating health care providers regarding the individual's medical conditions or opinions for submission in support of a claim for VA benefits.

(b) In response to such a request, VA treating health care providers must provide a statement or opinion describing the patient's medical condition, prognosis and degree of function.

(c) When the VA treating health care provider is the individual's treating provider and is unable, or deems it inappropriate, to provide an opinion or statement, such person must refer the request to another health care provider for the opinion or statement.

(d) If the Veteran requests that the form be sent directly to the requester (e.g., insurance company), the Veteran must sign VA Form 10-5345 prior to the disclosure being made.

(3) **Medical Opinions for Non-VA Purposes.**

(a) Individuals may also ask VA health care providers for opinions to assist them in filing claims with other agencies. For example, assistance may be provided for Family Medical Leave Act forms, life insurance application forms, non-VA disability retirement forms, State worker's compensation forms and State driver's license or handicapped parking forms.

(b) These opinions may be provided in the same manner and under the same restrictions as opinions furnished for VBA claim purposes.

(4) A CDC COVID-19 Vaccination Record Card is a medical form; therefore, a vaccination card for an individual can only be completed by a health care provider as a result of direct care or based on information contained in the VHA health record.

i. **Release of Name and Address.**

(1) The name and address of a patient or the patient's dependents, wherever found in medical or other records, must not be released without the patient's signed, written authorization, unless such disclosure is authorized by one or more of the disclosure provisions of the Privacy Act (see 38 C.F.R. §1.576(b)), 38 U.S.C. § 5701 and the HIPAA Privacy Rule.

(2) Any organization requesting a list of names and addresses of present or former patients and their dependents must make written application under the provisions of 38 C.F.R. §1.519 and VA Handbook 6300.6, Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses, dated October 21, 2015, to the Director, Privacy and Records Management Service at VA Central Office, 810 Vermont Avenue NW, Washington, DC 20420.

(3) Requests for lists of educationally disadvantaged Veterans must be addressed to the Director of the nearest VA Regional Office, as provided in 38 C.F.R. §1.519 and VA Handbook 6300.6.

(4) When a request is received from private organizations or individuals for names of patients for the purpose of distributing gifts, the facility Director may furnish names of patients only with the patients' prior written authorization.

(5) When disclosure of the patient's address is not permissible under the preceding paragraphs, the requester may be advised that a letter, enclosed in an unsealed envelope showing the name of the patient but no return address, and bearing sufficient postage, will be forwarded by VA (see 38 C.F.R. § 1.518(c)). Letters for the purpose of debt collection, canvassing or harassing a patient will not be forwarded.

j. **Release of Photographs and Information Concerning Individuals to the News Media.**

(1) Photographs and health information concerning individual patients may be released to news media with the signed, written authorization of the patient on VA Form 10-5345. In those instances where the patient has been declared legally incompetent, photographs or information may be released if written authorization of the court-appointed legal guardian has been obtained.

(2) Photographs and health information concerning individual patients in drug or alcohol abuse, HIV infection and sickle cell anemia treatment programs may be released to news media only with the prior signed, written special authorization of the individual, provided the authorization was given voluntarily and the disclosure would not be harmful to the individual.

(3) Before releasing any information to news media, the VA health care facility Public Affairs Office and the Public Affairs Guidelines are consulted.

(4) VHA may disclose information contained in the facility directory about a particular Veteran to the news media if the Veteran is an inpatient.

(5) VHA may disclose the minimum necessary information about a missing Veteran to the news media, at VHA's initiative, to assist in locating a missing patient when a determination has been made to notify the news media in accordance with 45 C.F.R. § 164.512(j)(1)(i). This information may include name, height, weight, hair color, clothing when last seen and a photograph, if available. Limited additional information may be disclosed where necessary to convey the urgency of the situation or to assist in handling the patient when located. For example, where appropriate, VHA may be able to disclose that a patient has Alzheimer's Disease and is a diabetic who needs to take their medicine immediately. No other personally identifiable information may be given. VHA may not, except as stated above, disclose diagnoses or other health information to the news media.

(6) **Employee Interviews.** The employee must obtain the appropriate approval in accordance with Public Affairs policy to speak to the news media. Employees are not authorized to disclose any personally identifiable information on a patient or Veteran during the interview without the prior signed, written authorization of the patient or Veteran. When an employee is asked to be interviewed by a third party, such as the news media, VA Form 10-3203a, Informed Consent and Authorization for Third Parties to Produce or Record Statements, Photographs, Digital Images or Video or Audio Recordings must be completed.

NOTE: *Photographs taken for treatment purposes are part of the patient's health record and are considered individually identifiable health information and do not require a separate consent form in accordance with VHA Directive 1078, Privacy of Persons Regarding Photographs, Digital Images, and Video or Audio Recordings, dated November 29, 2021.*

k. **Release of Information from Outside Sources.**

(1) Private hospital or health care provider records that have been incorporated into the individual's health records, whether through scanning of paper documents or through electronic means such as HIE, are considered part of VHA records and are subject to the disclosure provisions of the Privacy Act, the HIPAA Privacy Rule, 38 U.S.C. §§ 5701 and 7332 and FOIA.

(2) An individual, who is the subject of the record, requesting this type of record will be encouraged to obtain the information from the hospital or health care provider's office that is the original source of the information when the record is a paper or scanned document. However, if the individual insists on obtaining a copy from VHA, the request must be processed under the policies in this directive. For information incorporated into an electronic VHA record through HIE or other electronic means, the individual, who is the subject of the record, must be provided all information requested.

(3) Requests from third parties for information in the record except for the EHR that originated with another Federal agency must be referred to the agency that created the documents, if it is possible to ascertain the originating agency. The requester must be advised of the referral and whether the referring Federal agency will respond directly or that additional time will be needed for VA to consult with the other agency before a determination can be provided.

(4) Requests for PHI in the VA EHR from third parties will be processed in accordance with paragraphs 15-33 regardless of where the health information in the record originated.

(5) Information from health records of beneficiaries of other Federal agencies and allied governments treated or examined in VA health care facilities will be released to the subject of the record under paragraph 7 of this directive.

l. **Producing and Using Photographs, Digital Images or Video or Audio Recordings.**

(1) VHA must obtain an authorization from the patient or personal representative using VA Form 10-5345 prior to disclosing a photograph, digital image or video or audio recording if the product contains individually identifiable health information or PHI.

(2) Refer to VHA Directive 1078 for additional guidance on the production and use of photographs, digital images or video or audio recordings.

m. **Veteran Identification and Designation of Treatment Areas.**

(1) A VA health care facility may not request or require that a patient carry an identification card or possess any form of identification while away from the facility premises which would identify the individual as a patient being treated for drug abuse, alcoholism or alcohol abuse, HIV or sickle cell anemia.

(2) A VA health care facility may maintain cards, tickets or other devices to ensure positive identification of patients, correct recording of attendance or medication, or for

other proper purposes, provided that no pressure is brought on any patient to carry any device when away from the facility. Drug or alcohol abuse, HIV or sickle cell anemia patients may not be required to wear items including pajamas, robes or wrist bands that are different from other patients and which would identify them to VA health care facility staff or others as being treated for one or more of these conditions.

(3) Treatment locations are not to be identified by signs that would identify individuals entering or exiting these locations as patients enrolled in a drug or alcohol abuse, HIV infection or sickle cell anemia program or activity. Diagnostic names or names that suggest a diagnosis such as Dialysis Clinic or Diabetes Clinic must not be used. Naming conventions for clinics must be generic in nature such as colors or primary clinic, specialty clinic. VHA may maintain patient charts at bedside or outside of exam rooms, displaying patient names on the outside of patient charts, or displaying patient care signs (e.g., “high fall risk” or “diabetic diet”) at patient bedside or at the doors of inpatient hospital rooms.

(4) Bingo boards displaying patient name and bed number may be used as long as they are not visible in the hallway for visitors to view.

n. **Veterans Health Information Exchange.**

(1) In April 2009, President Obama directed VA and DoD to lead the efforts in creating the Virtual Lifetime Electronic Record, now referred to as the Veterans Health Information Exchange (VHIE), which would ultimately contain administrative and medical information from the day an individual enters military service, throughout their military career, and after they leave the military from both Federal agency and private sector provider organizations. The VHIE program office leads VHA's efforts for query-based exchange though national networks to securely share patient information with participating provider organizations.

(2) VHIE utilizes HIEs, such as eHealth Exchange and CommonWell, to share prescribed patient information via this protected network environment with participating private health care providers, but this does not involve ‘scanned’ patient information. The information shared is a pre-determined, standards-based set of clinical data that is sent to the requester. Direct access to the Veteran’s health record is not involved or authorized. Data exchanged through HIE is available for view via Joint Longitudinal Viewer (JLV) as read only and in the EHR joint electronic health record. Data may be added to the Veterans electronic record via manual entry, manual reconciliation or be auto-written if the source is approved.

(3) On April 18, 2020, VHIE moved to an informed Opt-Out Model, whereby all Veterans were automatically opted in for sharing their electronic health information unless they previously opted out. The change in policy to an Opt-Out Model was allowed by the VA MISSION Act of 2018, P.L. 115-182. Patients may opt-out of sharing by filing VA Form 10-10164 or opt-back-in by completing VA Form 10-10163, Request for and Permission to Participate in Sharing Protected Health Information through HIEs, on paper or electronically through MyHealth*e*Vet at any time. The VHIE Portal was then

implemented to replace the Veterans Authorizations and Preferences Portal and began sharing VA health information with DoD health information through the Oracle Cerner EHR via the Joint HIE. To accommodate Veteran requests for an accounting of electronic disclosures through HIE, please contact the VHIE Accounting of Disclosures Reporting mail group. ***NOTE:*** *For additional information about VHIE and the eHealth Exchange, go to: http://www.va.gov/vhie/.*

(4) Health information on deceased patients is only shared by VHIE through HIEs for treatment purposes for 180 days after date of death and never for benefits purposes after the date of death.

o. **Community Partners Supporting Homeless Veterans.**

(1) VHA Homeless Veteran program staff may disclose pertinent individually identifiable information, excluding 38 U.S.C § 7332-protected health information, to community partners, such as Supportive Services for Veteran Families (SSVF) and Grant and Per Diem (GPD) grantees, without a prior signed, written authorization from the Veteran for the purpose of obtaining critical services to prevent homelessness for the Veteran. VA considers homelessness in and of itself a serious and imminent threat to an individual; therefore, when a Veteran is known to be homeless or at a high risk of homelessness, such as in a shelter or in temporary/transitional housing, authority to disclose exists.

(2) VHA may disclose individually identifiable information, excluding 38 U.S.C. § 7332-protected information, to community partners, such as SSVF and GPD grantees, for referrals to lessen the threat associated with the Veteran's homelessness or risk of homelessness. VHA staff must complete the Referral Packet using information from HOMES, which is part of the VHA Privacy Act System of Records 121VA10A7, National Patient Data bases-VA, and the authority for the disclosure under the Privacy Act is a routine use.

37. GENERAL OPERATIONAL PRIVACY REQUIREMENTS

a. **Designation of Privacy Officer.**

(1) VHA must retain a full-time Privacy Officer.

(2) Each VA medical facility must designate at least one facility full-time Privacy Officer who must report to and be supervised by the VA medical facility Director, the VA medical facility Associate Director, the VA medical facility Assistant Director or a senior individual who reports directly to and is supervised by the VA medical facility Director, Associate Director or Assistant Director and whose primary responsibilities at the facility include privacy program responsibilities. The VA medical facility Privacy Officer must be able to raise privacy issues and concerns directly to the Director, Associate Director or Assistant Director regardless of Supervisor to ensure appropriate awareness and accountability.

(a) No collateral duties other than FOIA and privacy-related duties may be assigned to the VA medical facility Privacy Officer. The VA medical facility FOIA Officer and the VA medical facility Privacy Officer may be but are not required to be the same person.

(b) The VA medical facility Privacy Officer is not a position suitable to be 100% remote or virtual. Teleworking is acceptable on an as needed basis but all responsibilities that require the VA medical facility Privacy Officer to be onsite need to be considered.

(3) Each VHA program office must have a designated Privacy Officer or Liaison to coordinate privacy activities of their VHA program office with the VHA Privacy Office.

(4) All other facilities not discussed in the above paragraphs must have a designated Privacy Officer which may be a collateral duty and based on supervisory discretion may be virtual.

b. **Management of Release of Veteran Information.**

(1) ROI from the Veteran's health record is a complex function, requiring trained and qualified employees and expert guidance. At a VA medical facility, the management function must be assigned to the facility Chief, HIM. ***NOTE:*** *For other VA health care facilities, release of individually identifiable information on Veterans may be managed by the Data Owner but the Facility Privacy Officer must be consulted prior to disclosure*.

(2) ROI must provide for the timely release as outlined in paragraph 15.b. in accordance with written requests for information received by VHA. ROI staff at VA medical facilities must use ROI Plus or other designated ROI software to manage and track requests and generate the accounting of disclosures. To ensure timely and informed ROI, it is recommended that all requests be processed through a central point within the VA medical facility.

(3) For a VA medical facility, the Chief of HIM or Privacy Officer must monitor the Turn-Around Report (TAT) from ROI Plus or other designed ROI software to identify backlogs and expedite responses to requests for information. For instructions for running the TAT Report in ROI Plus, see the ROI Plus Administrative Manual located at https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/roi.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

(4) ROI staff may only disclose or release Veteran health records in accordance with this directive. Chief Counsel must be consulted when a legal opinion is needed concerning the release of a Veteran's individually identifiable health information (e.g., subpoenas, court orders, powers of attorney or Veteran incompetency).

c. **Complaints.**

(1) Only individuals who are the subject of individually identifiable information, including PHI, or their personal representative have the right to file a complaint

regarding VHA privacy policies or practices. The complaint does not have to be in writing, though it is recommended.

(2) Complaints are to be forwarded to the appropriate Facility Privacy Officer or designee or the VHA Privacy Office, 810 Vermont Avenue NW, Washington, DC 20420.

(3) All individuals filing a privacy complaint are to be provided with the Notice to Privacy Complainants, IB 10-686, at the time of the complaint submission. If the complaint is made verbally, the Facility Privacy Officer or designee or the VHA Privacy Office shall try to obtain mailing or email information in order to send the privacy complainant the Notice. The Notice must be mailed or emailed out within 5 business days if the Notice is not given in person. A cover letter must be included when the Notice is mailed or emailed.

(4) All privacy complaints, regardless of validity, must be:

(a) Documented in the tracking service designated by the VA Data Breach Response Service (e.g., PSETS) by the Facility Privacy Officer within 1 hour of receiving the notification or discovery by the Facility Privacy Officer. ***NOTE:*** *Notification and created time must always be within 1 hour of each other in PSETS. Create time in PSETS defaults to midnight if not changed by the Facility Privacy Officer.* The complaint must be changed in PSETS to an incident if the complaint is determined to be valid after the fact-finding is complete,

(b) Communicated to leadership, as appropriate (e.g., Facility Director, VISN Director, VHA Privacy Office, OIG, OGC),

(c) Reviewed and investigated promptly and documented in PSETS, and a file must be kept including interviews of involved parties and reports of contact requested, as outlined in paragraph 37.d.,

(d) Provide documented outcomes and findings to the VHA supervisor and coordinated with stakeholders (e.g., HR for sanctions or disciplinary actions, union representatives, department heads), and

(e) Managed to full resolution and closure upon notification from the Data Breach Resolution Service in PSETS.

(5) A written response must be provided to the privacy complainant as soon as possible or no later than 60 calendar days, explaining the results of the fact-finding for all privacy complaints. If the fact-finding process cannot be completed within 60 calendar days due to the volume of allegations, such as with unauthorized access, an interim written response must be provided informing the privacy complainant of the delay and any findings currently available. ***NOTE:*** *A fact-finding for a privacy complaint may never go beyond 180 calendar days.*

(6) When the privacy complaint alleges unauthorized access and it cannot be proven that the access is likely, or more likely than not, authorized, the access must be presumed to be unauthorized.

(7) When an individual requests their Sensitive Patient Access Report (SPAR) from VistA or Access Audit Log from P2Sentinel, it will be provided as the report and log are part of a Privacy Act System of Records. If a complainant does not give a period of time for the running of the SPAR or Access audit log, the VA medical facility Privacy Officer will ask the individual for the desired timeframe. If the individual wants the SPAR or Access audit log for the entire timeframe for which it exists, then it would be provided as such under Right of Access. A complainant cannot return a SPAR or Access audit log to the VA medical facility Privacy Officer without pointing out which accesses they would like investigated. A returned SPAR or Access audit log without any accesses highlighted will not be accepted. ***NOTE:*** *Responses to the complainant may be emailed if encrypted using encryption software such as RMS AZURE.*

(8) Facility Privacy Officers must trend the types of privacy complaints identified and report these trends to the facility leadership twice a year and to the VHA Privacy Office upon request.

(9) Facility Privacy Officers must cooperate with auditing entities and provide all required documentation for privacy complaints, regardless of validity, in accordance with VA Directive 6502.

(10) The VHA Privacy Office serves as the central authority for coordination of HHS-OCR privacy and security complaints received by all VA health care facilities. Any HHS-OCR privacy or security complaints received by VA health care facilities must be forwarded to the VHA Privacy Office. If the Facility Privacy Officer receives a HHS-OCR notification letter, this notification letter must be forwarded via encrypted email to VHAPrivIssues@va.gov.

(a) Facilities must work with the VHA Privacy Office to ensure a complete response is provided to HHS-OCR within 60 calendar days or within the timeframe specified by HHS-OCR. The Facility Privacy Officer functions as a liaison between facility staff and the VHA Privacy Office.

(b) HHS-OCR complaints must be treated as priority by facility staff and failure to cooperate with the VHA Privacy Office in an HHS-OCR inquiry will result in escalation to the VA health care facility leadership.

(11) An individual has 3 years from the date of the privacy violation or concern to file a privacy complaint regarding their individually identifiable information with VHA unless good cause to extend the timeframe based on the judgement of the Facility Privacy Officer is shown. HHS-OCR only accepts privacy complaints filed within 180 days of when the complainant knew that the act or omission complained about occurred. HHS-OCR may extend the 180-day period if the complainant can show good cause (45 C.F.R. § 160.306). ***NOTE:*** *Failure of an individual to obtain and review their SPAR or*

Access audit log that exists in order to identify an alleged privacy violation is not good cause to extend the timeframe for submitting a privacy complaint.

(12) Privacy incidents are investigated in a similar manner to privacy complaints. Privacy events submitted by VA employees who are not the subject of the information in question may only be treated as privacy incidents. For more complete information about investigating complaints and incidents see the Guide to Investigating Privacy Events in VHA, available at: https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/FactSheets.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

(13) There is no privacy complaint appeal process beyond the right of the individual to file the same complaint with the VHA Privacy Office or HHS-OCR. A VA medical facility Privacy Officer must not reconduct a fact-finding or reinvestigate a privacy complaint unless directed to do so by the VHA Privacy Office.

d. **Privacy Complaint File.**

(1) The Privacy Complaint File is the facility's complete documentation of events and actions taken to investigate all privacy complaints, incidents and breaches. The complaint file is considered the investigative file in the instance that an outside agency would request information pursuant to a privacy complaint by an individual. All privacy complaints must be documented regardless of validity. Documentation in the complaint file includes:

(a) Initial written (e.g., email or handwritten) concern or issue from complainant or a written Report of Contact by the Facility Privacy Officer, if the complaint is made verbally. This documentation must include the submission date of the privacy complaint. The privacy complaint may be filed by either the submission date or the PSETS ticket number.

(b) Description of steps taken, or process followed when investigating the complaint and what lead to determining the validity of the complaint or if there was a privacy violation.

(c) List of who was interviewed during the investigation, their title and their role in the privacy investigation process. This documentation must also include:

1. A standard list of questions used during the investigation and interviewee responses to those questions.

2. If no standard list of questions is used, the file must contain a brief summary of the interview including general information about the interviewee(s) and their responses.

(d) Facility Privacy Officer's official recommendations to HR and the VA employee's supervisor for potential sanctions actions from the table of penalties to ensure standard sanctions are applied.

(e) Any additional correspondence with the complainant or other individuals involved in the investigation that were contacted by the Facility Privacy Officer. This may include the VA medical facility ISSO, VA Police and Security and the Office of Regional Counsel.

(f) Copies of the signed final complaint response letters and correspondence with the complainant and affected individuals.

(g) A copy of the PSETS ticket and determination of the VA Data Breach Resolution Service and Data Breach Core Team (DBCT) must be kept with the complaint file when a privacy violation is determined by the DBCT to be a data breach. When the DBCT determines the privacy violation to be a data breach as outlined in VA Handbook 6500.2, then a listing of all affected individuals receiving notification letters or credit monitoring must be maintained with the complaint file. Any other actions required by the Facility Privacy Officer as a result of sending notification or credit monitoring letters as required by VA Handbook 6500.2 must also be part of the complaint file.

(2) Records Maintenance of the Privacy Complaint File. The Privacy Complaint File must be maintained and disposed of according to RCS 10-1, which allows the file to be destroyed 3 years after resolution or referral, as appropriate, but authorizes longer retention if required for business use. Since the HIPAA Privacy Rule at 45 C.F.R. § 164.530(j) requires VHA to retain complaint documentation for 6 years from the date of its creation, longer retention is required in order to meet this requirement. As such, Privacy Complaint Files must be retained for 6 years from the date of the last agency response letter to the complainant or HHS-OCR, whichever is later.

e. **Whistleblower.**

(1) The Whistleblower Protection Act protects employees who report alleged violations of law, rule or regulation, or gross mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to public health or safety. However, while the Act generally protects whistleblowers when they submit such allegations to VA OIG, OSC or Congress, it does not free VA employees from their obligation to safeguard personally identifiable information, including PHI, to the extent it is protected from disclosure by other privacy laws or regulations. ***NOTE:*** *VA personnel are permitted to share personally identifiable information or PHI to report concerns or allegations of violations of law with their VHA leadership, supervisor or other VHA program offices responsible for compliance and accountability (e.g., ORO).*

(2) A whistleblower who believes that VHA has engaged in conduct that is unlawful or otherwise violates professional or clinical standards or that the care, services or conditions provided by VHA potentially endangers one or more patients, workers or the public, may always disclose personally identifiable information and PHI to VA OIG and Congressional Committees (e.g., House Veterans Affairs Committee and Senate Veterans Affairs Committee) authorized by law to investigate or otherwise oversee the relevant conduct or conditions of VHA. ***NOTE:*** *Individual Members of Congress are not covered.*

(3) A whistleblower may disclose any personally identifiable information or PHI, except information protected by 38 U.S.C. § 5705 (Medical Quality Assurance Information) and 38 U.S.C. § 7332 (HIV, sickle cell anemia, drug and alcohol treatment) to OSC for the purpose of reporting the allegation of misconduct by VHA.

(4) A whistleblower may disclose any personally identifiable information or PHI, except Veterans' names and addresses protected by 38 U.S.C. § 5701 and information protected by 38 U.S.C. § 5705 and 38 U.S.C. § 7332 to a public health authority authorized by law to investigate the relevant conduct of VHA employees or an appropriate health care accreditation organization with whom VHA has a relationship, such as The Joint Commission, for the purpose of reporting the allegation of failure to meet professional standards or misconduct by VHA.

(5) VA personnel who disclose personally identifiable information or PHI to an entity other than as permitted above may be considered to have made an unauthorized disclosure in violation of the Privacy Act, 38 U.S.C. § 5701, 38 U.S.C. § 5705, 38 U.S.C. § 7332, HIPAA Privacy Rule or VHA policy. Such unauthorized disclosure may result in disciplinary action.

(6) Whistleblower retaliation is not tolerated in VA. It is a prohibited personnel practice for an agency to subject an employee to a personnel action if the action is threatened, proposed, taken or not taken because of whistleblower activities.

(7) If VHA receives a privacy complaint that an employee disclosed information under a potential whistleblower activity, HRMS, Chief Counsel or VHA Privacy Office must be consulted to determine whether privacy legal authority existed for the disclosure.

f. **Faxes.**

(1) Fax machine transmittals may be used when no other means exists to provide the requested information in a reasonable manner or time frame and the receiving fax machine is in a secure location and reasonable steps (e.g., verifying the fax number and notifying the individual prior to faxing) have been taken to ensure the fax transmission is sent to the appropriate destination and will be secured promptly upon arrival.

(2) Fax machine transmittals may be used for non-patient care; however, all established fax protocols must be strictly observed.

(3) A confidentiality statement must be attached to the cover page when transmitting individually identifiable health information. For example, when transmitting outside VA:

"This fax is intended only for the use of the person or office to which it is addressed and may contain information that is privileged, confidential, or protected by law. All others are hereby notified that the receipt of this fax does not waive any applicable privilege or exemption for disclosure and that any dissemination, distribution, or copying of this communication is prohibited. If you have received this fax in error, please notify this office immediately at the telephone number listed above."

(4) PHI is not to be written on the fax cover sheet, only the Veteran's name for identification purposes. All PHI must be within the documents under the fax cover sheet.

NOTE: *For further information, see VA Handbook 6500.*

g. **Miscellaneous Electronic Topics.**

(1) Electronic mail (email) and information messaging applications and systems are to be used as outlined in VA Handbook 6500.

(2) Email messages must not contain personally identifiable information or PHI, unless the data is encrypted using public key infrastructure encryption software such as RMS Azure.

(3) Email communication with Veterans may only occur with policy approval from appropriate VHA program offices overseeing the purpose of the communication. For example, Revenue Operations would need to permit billing communications. Researchers must have IRB, if applicable per VHA Directive 1200.05(3), and the R&D Committee approval prior to email communication with Veterans. Provider-Veteran communication for any other purposes must use secure messaging through MyHealtheVet.

(4) **Last Four Digits of SSN.** VA OGC has determined that the last four digits of SSN and first initial of the last name are not unique identifiers of a single individual by themselves. However, if any other personally identifiable information or health information is added within the message, or health information that has not been de-identified in accordance with this directive, the sender may no longer send this alpha-numeric code via Microsoft (MS) Outlook email without encryption.

(5) **Subject Line.** The first initial of the last name and last four digits of the SSN by themselves can be included in the subject line of an email message only if no other identifying information is contained there.

(6) **Outlook Calendar.** It is not acceptable to include PHI in the MS Outlook calendar. The MS Outlook calendar may be placed on a shared drive with PHI as long as:

(a) Access to the data is controlled to only those who require access.

(b) Access is monitored and audited regularly to ensure only those who need access have access.

(c) Information that is no longer needed is removed from the site within 90 days.

(7) **MS Teams.** Personally identifiable information, including health information, may be shared using MS Teams as the platform is secure; however, there are constraints around the storage and access to personally identifiable information shared through MS Teams. Personally identifiable information must only be shared using MS Teams with

VHA personnel who have a need for this information in the performance of their official duties. Before sharing personally identifiable information using MS Teams, consulting the VA medical facility Privacy Officer is encouraged to ensure need to know exists and processes exist to address the constraints.

h. **Contracts.**

(1) All contracts must meet contracting requirements as dictated by VA's Office of Acquisition and Material Management and the Federal Acquisition Regulations (FAR).

(2) Any contract between VHA and a contractor for the design, development, operation or maintenance of a VHA Privacy Act System of Records, or any contract that necessitates the use of personally identifiable information, must conform to VA Handbook 6500.

(3) Organizations with whom VHA has a contract for services on behalf of VHA, where individually identifiable health information is provided to or generated by the contractors, may be considered Business Associates. ***NOTE:*** *For additional information on Business Associates see the HIA website:* http://vaww.vhadataportal.med.va.gov/PolicyAdmin/BusinessAssociateAgreements.aspx. *This is an internal VA website that is not available to the public.*

(4) Business Associates must follow VHA Directive 1605.05.

(5) All contractors and Business Associates must receive privacy training annually and the contract or BAA must include this requirement.

(a) For contractors and Business Associates who do not have access to PHI in VHA computer systems, such as JLV or the EHR, this requirement is met by receiving the VA Privacy and Information Security Awareness and Rules of Behavior training or other contractor furnished training that meets the requirements set forth by VA. Proof of training is required.

(b) For contractors and Business Associates who are granted access to PHI in VHA computer systems, such as JLV or the EHR, this requirement is met by receiving the Privacy and HIPAA training or other contractor furnished training that meets the requirements set forth by VHA. Proof of training is required.

(6) The Facility Privacy Officer is responsible for reviewing the Statement of Work and the VA Handbook 6500.6 Contract Security checklist to determine if there is VA sensitive information and if a BAA is needed. The Facility Privacy Officer must work collaboratively with the ISSO and Contracting Officer to ensure the checklist is completed accurately and timely. The Facility Privacy Officer will not sign a blank checklist nor are they be the subject matter expert for the checklist. If the contract does not involve the use, collection or sharing of VA sensitive information and the contract is only for a purchase order, then the Facility Privacy Officer is not required to sign off on the checklist.

(7) The Facility Privacy Officer must determine what privacy requirements under VA Handbook 6500.6 are required for the contract.

i. **Penalties to an Individual.**

(1) **Violations of the Privacy Act.**

(a) A VA employee who knowingly and willfully violates the provisions of 5 U.S.C. § 552a(i) is guilty of a misdemeanor and can be fined not more than $5,000 when the employee:

1. Knows that disclosure of records which contains individually identifiable information is prohibited and willfully discloses the information in any manner to any person or agency not entitled to receive it,

2. Willfully maintains records concerning identifiable individuals that have not met the Privacy Act notice requirements, or

3. Knowingly and willfully requests or obtains any record concerning an individual from VA under false pretenses. ***NOTE:*** *This requirement only applies to persons who are not VA employees.*

(b) In the event a VA health care facility employee is found criminally liable of a Privacy Act violation, a written report of the incident must be provided to the VA medical facility Director.

(2) **Violation of 38 U.S.C. § 7332.** Any person who violates any provision of 38 U.S.C. § 7332 can be fined not more than $5,000 in the case of a first offense, and not more than $20,000 in any subsequent offense (38 U.S.C. § 7332(g)).

(3) **Violation of HIPAA (42 U.S.C. § 1320d-6).** Any person who knowingly violates the provisions of HIPAA by using a unique health identifier, obtaining personally identifiable information or disclosing individually identifiable health information to another person can be fined not more than $50,000, imprisoned not more than 1 year, or both, unless:

(a) The offense is committed using false pretenses, then the person can be fined not more than $100,000, imprisoned not more than 5 years, or both, or

(b) The offense is committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm, then the person can be fined not more than $250,000, imprisoned not more than 10 years, or both.

(4) **Administrative or Disciplinary Actions.** In addition to the statutory penalties for the violations described in paragraph 38.i., administrative actions or disciplinary or other adverse actions (e.g., admonishment, reprimand or termination) may be taken against

employees who violate the Privacy Act, 38 U.S.C. § 7332 and HIPAA Privacy Rule statutory provisions.

j. **VA Forms.**

(1) The Social Security Number Fraud Prevention Act of 2017, 42 U.S.C. § 405 Note, prohibits the inclusion of SSNs on any document or item sent by mail unless the head of the agency determines that the inclusion of the SSN is necessary.

(2) Any VA form that requests individuals to supply personal information on the form must contain a Privacy Statement in accordance with VA Directive 6310, Forms, Collections of Information, and Reports Management, dated December 1, 2001, and the Privacy Act, 5 U.S.C. § 552a(e). The Privacy Statement must include:

(a) The authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary.

(b) The principal purpose or purposes for which the information is intended to be used.

(c) The routine uses which may be made of the information, as published in the VHA Privacy Act Systems of Records.

(d) The effects on the individual, if any, of not providing all or any part of the requested information.

(3) If the VA form collects SSN and is not mailed out, the Privacy Statement must also indicate whether the disclosure of the SSN is voluntary or mandatory. The person must also be told that VA is requesting the SSN under the authority of title 38 United States Code. The person must also be told that it will be used in the administration of Veterans' benefits in the identification of Veterans or persons claiming or receiving VA benefits and their records, and that it may be used to verify social security benefit entitlement (including amounts payable) with SSA and, for other purposes where authorized by both title 38 United States Code and the Privacy Act.

k. **Agency Accounting of Disclosure Requirements.**

(1) VA health care facilities and programs are required to keep an accurate accounting for each disclosure of an individual’s record, including State reporting and research. An accounting is not required to be maintained in the following situations when the disclosure is:

(a) To VA employees who have a need for the information in the performance of their official VA job duties,

(b) Pursuant to a FOIA request,

(c) To an individual under Right of Access, or

(d) Of a limited data set or de-identified data.

(2) The accounting must be maintained by VHA for 6 years after the date of disclosure or for the life record disclosed (see RCS 10-1), whichever is longer and must include all of the following:

(a) The name or other unique identifier of the individual to whom the information pertains.

(b) The date of each disclosure.

(c) Nature or description of the individually identifiable information disclosed.

(d) Purpose of each disclosure.

(e) Name and, if known, address of the person or agency to whom the disclosure was made.

(3) The accounting record may be maintained via a VHA-approved tracking system or manually, such as on VA Form 5572, Accounting of Records/Information Disclosure Under the Privacy Act, or an Excel spreadsheet. The accounting record does not have to be generated in real-time or contemporaneously with the disclosure. The accounting record may be generated retrospectively as long as all of the required elements can be compiled to create the accounting of disclosures upon request.

(4) For disclosures made from the VHA Privacy Act System of Records, Patient Medical Record-VA (24VA10A7) through ROI, VA medical facilities must use the ROI Plus software to account for disclosures as required by VHA Directive 1615.

l. **Flagging Patient Records Sensitive.**

Some health records of patients are deemed sensitive requiring the flagging as “sensitive” in VistA for tracking of accesses to those patients’ records. Some patients are flagged by VA and these patients are:

(1) All VA employees.

(2) Regularly scheduled official VA volunteers who are Veterans.

(3) Veterans whose records are involved in tort claim activities concerning VA.

(4) Veteran fugitive felons.

(5) Veterans or patients with complaints of unauthorized access to their health record.

(6) Identified high-profile Veterans or patients where tracking of access is warranted.

(7) Other patients upon their request must be flagged and these patients are:

(a) Active duty Service member.

(b) Other Federal employees (e.g., DoD staff).

(c) VA contractors.

(d) Publicly elected officials who are Veterans.

NOTE: *With the concurrence of the VA medical facility Privacy Officer and ISSO similar security measures for the tracking of access may be applied to other patient records.*

38. TRAINING

a. All VHA personnel must be trained, at least annually, on privacy policies to include the requirements of Federal privacy and information laws, regulations and VHA policy. The Talent Management System (TMS) VA-10203: Privacy and HIPAA Training is one option for meeting the training mandate and is updated annually on October 1 to reflect changes to guidance.

b. Newly hired personnel must complete privacy training within 30 days of employment. If personnel have access to PHI, they are required to take the TMS VA-10203: Privacy and HIPAA Training or equivalent VHA Privacy Office-approved privacy training based on their role.

c. If personnel, including contractors and Business Associates, do not have access to PHI, but they have access to VA computer systems they must take VA Privacy and Information Security Awareness and Rules of Behavior.

d. If personnel do not have access to VA computer systems or direct access to PHI, they can take the VA Privacy Training for Personnel without Access to VA Computer Systems. This training is available in the TMS.

e. At a minimum, instruction must be provided within 6 months of significant change in Federal law, regulation, this directive, or VA health care facility or office procedures.

f. VA health care facilities must work in collaboration with TMS coordinators to track completion of privacy training.

g. Contractors and Business Associates with access to PHI must complete the Privacy and HIPAA training if their training does not comply with VHA privacy policy requirements.

h. VA Handbook 6500 outlines the consequences if a user does not engage in or cannot meet general or specialized training requirements.

39. RECORDS MANAGEMENT

All records regardless of format (e.g., 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 RCS 10-1. Questions regarding any aspect of records management should be addressed to the appropriate Records Officer.

40. BACKGROUND

a. As a Federal Government agency and as a health plan and health care provider, VHA must comply with all applicable privacy and confidentiality statutes and regulations. The most commonly encountered statutes and sets of regulations are identified in paragraph 40.b. and addressed by this directive. Questions concerning legal confidentiality and privacy requirements not covered in this directive must be addressed to OGC or one of OGC's Offices of Chief Counsel in the Districts (Chief Counsel). Generally, the same privacy rules apply across VA. However, regulations promulgated by HHS under the HIPAA Privacy Rule of 1996 impose additional requirements on VHA's privacy practices for PHI. HIPAA regulations impose specific requirements for VHA to act, in certain circumstances, as a separate entity from the rest of VA. This directive provides these requirements and addresses how VHA simultaneously satisfies the requirements of these regulations and other confidentiality requirements established by statute or regulation.

b. The six statutes (and their implementing regulations) that govern the collection, maintenance and ROI from VHA records are:

(1) **The Freedom of Information Act, 5 U.S.C. § 552, implemented by 38 C.F.R §§ 1.550-1.562.** FOIA compels disclosure of reasonably described VHA records or a reasonably segregated portion of the records to any individual upon written request, unless the requested records or portions thereof must be withheld under one or more of nine exemptions apply to the records (see 5 U.S.C. § 552(b)(1)-(b)(9) and 38 C.F.R. § 1.554(a)(1)-(9)). A FOIA request may be made by any individual (including foreign citizens), partnerships, corporations, associations and foreign, State or local governments. Federal employees acting in their official capacities and Federal agencies may not make FOIA requests for VHA records. VHA administrative records should be made available to the greatest extent possible in keeping with the spirit and intent of FOIA. All FOIA requests must be processed in accordance with 5 U.S.C. § 552; 38 C.F.R. §§ 1.550-1.562; VA Directive 6213, Freedom of Information Act (FOIA), dated September 15, 2021; and VHA Directive 1935.

(2) **The Privacy Act, 5 U.S.C. § 552a, implemented by 38 C.F.R. §§ 1.575-1.582.** Generally, the Privacy Act provides for the confidentiality of personally identifiable information about living individuals retrieved by name or another unique identifier. VHA must maintain this information according to the terms of a published Privacy Act System of Records and may disclose Privacy Act-protected records only when specifically authorized by the statute. The Privacy Act provides that VHA may collect information

about individuals for a purpose that is legally authorized, relevant and necessary for VHA to perform its statutory duties. All personally and individually identifiable information must be maintained in a manner that precludes unwarranted intrusion upon individual privacy. Information is collected directly from the individual to the extent possible. At the time information is collected, the individual must be informed of the authority for collecting the information, whether providing the information is mandatory or voluntary, the purposes for which the information will be used and the consequences of not providing the information. The Privacy Act requires VHA to take reasonable steps to ensure that its Privacy Act-protected records are accurate, timely, complete and relevant. ***NOTE:*** *The information collection requirements of the Paperwork Reduction Act of 1995 (44 U.S.C. §§ 3501-3521) must be met, where applicable.*

(3) **The VA Claims Confidentiality Statute (formal title, Confidential Nature of Claims), 38 U.S.C. § 5701, implemented by 38 C.F.R. §§ 1.500-1.527.** 38 U.S.C. § 5701 provides for the confidentiality of all VA files, records, reports and other papers and documents that pertain to any VA claim, the name and address of present or former personnel of the armed services and their dependents and permits disclosure of such information only when specifically authorized by the statute. ***NOTE:*** *Veterans' and caregivers' health records generated and maintained by VHA pertain to claims for VA health care benefits*.

(4) **Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus Infection and Sickle Cell Anemia Health Records, 38 U.S.C. § 7332, implemented by 38 C.F.R. §§ 1.460-1.496.** Section 7332 of title 38 U.S.C. provides for the confidentiality of certain individually identifiable patient health information about the identity, diagnosis, prognosis or an offer or referral for treatment of drug and alcohol abuse, alcoholism treatment of sickle cell anemia or HIV infection. Section 7332 permits disclosure of the protected information only when specifically authorized, in writing, by the patient or legal guardian; or personal representative as authorized by the patient; or by the common disclosure provisions of this statute or its implementing regulations.

(5) **HIPAA (P.L. 104-191), implemented by 45 C.F.R. Parts 160 and 164.** HIPAA provides for the improvement of the efficiency and effectiveness of health care systems by encouraging the development of health information systems through the establishment of standards and requirements for the electronic transmission, privacy and security of certain health information. Most of the privacy requirements are contained in the implementing regulations, which are referred to in this directive as the HIPAA Privacy Rule. VHA must comply with the HIPAA Privacy Rule when creating, maintaining, using and disclosing individually identifiable health information. All individually identifiable health information on Veterans and caregivers maintained by VHA is considered PHI under the HIPAA Privacy Rule.

(6) **Confidentiality of Medical Quality Assurance Review Records, 38 U.S.C. § 5705, implemented by 38 C.F.R. §§ 17.500-17.511.** This statute provides that records and documents created by VHA as part of a designated medical quality-assurance program are confidential and privileged and may not be disclosed to any person or

entity except when specifically authorized by 38 U.S.C. § 5705 or its implementing regulations.

c. When following VHA policies, all six statutes will be applied simultaneously in order to decide how to proceed. VA health care facilities need to comply with all statutes, so that the result will be the application of the more stringent provision for all uses or disclosures of VA health care data and in the exercise of the greatest rights of the individual. For example, when an individual is exercising their right of access and requests a copy of the individual's own records, VHA must provide the records to which the individual would be entitled under the Privacy Act, FOIA and the Right of Access under the HIPAA Privacy Rule. VHA may refuse to provide a copy of the records only where the individual is not entitled to them under all of these legal authorities. ***NOTE:*** *De-identified information is not considered to be individually identifiable; therefore, the Privacy Act, HIPAA and VA confidentiality statutes 38 U.S.C. §§ 5701 and 7332 do not apply; only FOIA still applies (see Appendix A).*

41. DEFINITIONS

NOTE: *The terms defined below are contained in statutes or regulations. The following definitions are intended to have the same meaning contained in the statutes and regulations, unless otherwise specified, and are meant to be easy to understand without changing the legal meaning of the term.*

a. **Access.** Access is the obtaining or using of information, electronically, on paper, or through other medium, for the purpose of performing an official function.

b. **Accounting of Disclosure.** An accounting of disclosure is a list of all disclosures made to entities outside the VA. This is not the same as the SPAR.

c. **Amendment.** An amendment is the authorized alteration of an individual's health information by modification, correction, addition or deletion at the request of the individual.

d. **Business Associate.** A Business Associate is an entity, including an individual, company or organization that performs or assists in the performance of a function or activity on behalf of VHA that involves the creation, receiving, maintenance or transmission of PHI, or that provides to or for VHA certain services as specified in the HIPAA Privacy Rule that involve the disclosure of PHI by VHA. Subcontractors of Business Associates are also considered Business Associates.

e. **Claimant.** A claimant is any individual who has filed a claim for disability benefits under 38 U.S.C. § 5101, including health benefits, under 38 C.F.R. part 17.

f. **Close Friend.** A close friend is any person 18 years or older who has shown care and concern for the patient's welfare, who is familiar with the patient's activities, health, religious beliefs and values and who has presented a signed written statement for the record that describes that person's relationship to and familiarity with the patient.

g. **Compensated Work Therapy Workers.** A CWT worker is a patient in an inpatient treatment program who is compensated by VHA. CWT workers are not VHA employees. CWT workers cannot have access to or work in areas where they will be exposed to personally identifiable information. VHA may not disclose or release any PHI to a CWT Worker without the signed written authorization of the individual to whom the information pertains.

h. **Contractor.** A contractor is a person who provides services to VA such as data processing, dosage preparation, laboratory analyses or medical or other professional services. Each contractor must be required to enter into a written agreement subjecting such contractor to the provisions of 38 C.F.R. § 1.460 through 1.499, 38 U.S.C. §§ 5701 and 7332 and 5 U.S.C. § 552a and 38 C.F.R. § 1.576(g).

i. **Court Order.** A court order is a written directive or mandate, signed by a court or judge, directing that some action be taken or prohibiting some action being taken. A subpoena is only a court order if it is signed by a judge.

j. **De-identified Information.** De-identified Information is health information that is presumed not to identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual, because the 18 patient identifiers described in the HIPAA Privacy Rule have been removed or a qualified biostatistician has determined that the health information has been de-identified. De-identified information is no longer covered by the Privacy Act, 38 U.S.C. § 5701, 38 U.S.C. § 7332 or the HIPAA Privacy Rule. See Appendix A.

k. **Designated Record Set.** A designated record set is a group of records, maintained by or for VHA, that are the health records and billing records; enrollment; payment; claims; adjudication; case or medical management records; or records used, in whole or part, to make decisions regarding individuals. For the purposes of this directive, all designated record sets are covered under a Privacy Act System of Records.

l. **Disclosure.** Disclosure is the release, transfer, provision of access to, or divulging in any other manner, including verbally, information to an entity or individual outside VHA. Once information is disclosed VHA may choose to retain ownership of the data, such as per an agreement, or may be required to retain ownership, such as when to a Business Associate or contractor. In most cases VHA relinquishes ownership of the information upon disclosure. The exception to this definition is when the term is used in the phrase “accounting of disclosures.”

m. **Electronically Created and Authenticated Signature.** An electronically created and authenticated signature is a signature that meets the following requirements: 1) An appropriate means to identify and authenticate the signer; 2) The electronic form of signature must be executed or adopted by the signer with the intent to sign the electronic record; 3) The electronic form of signature must be attached to or associated with the electronic record being signed; and 4) There must be a means to preserve the integrity of the signed record.

n. **Electronic Health Record.** EHR is the digital collection of patient health information resulting from clinical patient care, medical testing and other care-related activities. Authorized VA health care providers may access EHR to facilitate and document medical care. EHR comprises existing and forthcoming VA software including CPRS, VistA and Cerner platforms. ***NOTE:*** *The purpose of this definition is to adopt a short, general term (EHR) to use in VHA national policy in place of software-specific terms while VA transitions platforms.*

o. **Facility Privacy Officer.** A Facility Privacy Officer is an individual designated as a Privacy Officer for a VHA program office, VISN, VA medical facility or VA health care facility, including Vet Centers.

p. **Family Member.** Family member includes, but is not limited to, the spouse, parent, child, step-family member, extended family member and any individual who lives with the Veteran but is not a member of the Veteran's family.

q. **Fiduciary.** For purposes of this directive, a fiduciary is a person who is a guardian, curator, conservator, committee or person legally vested with the responsibility or care of a claimant (or a claimant's estate) or of a beneficiary (or a beneficiary's estate); or any other person having been appointed in a representative capacity to receive money paid under any of the laws administered by the Secretary of Veterans Affairs for the use and benefit of a minor, incompetent or other beneficiary.

r. **Genetic Information.** Genetic information, with respect to an individual, means information about: (1) the individual's genetic tests, (2) the genetic tests of the individual's family members, (3) the manifestation of a disease or disorder in the individual's family members or (4) any request for, or receipt of, genetic services or participation in clinical research which includes genetic services, by the individual or any of the individual's family members. Genetic information is health information.

s. **Genetic Services.** Genetic services are genetic tests, genetic counseling (including obtaining, interpreting or assessing genetic information) or genetic education.

t. **Genetic Test.** A genetic test is an analysis of human DNA, RNA, chromosomes, proteins or metabolites, if the analysis detects genotypes, mutations or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder or pathological condition.

u. **Health Care Operations.** Health care operations are any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 C.F.R. § 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care

providers and patients with information about treatment alternatives; and related functions that do not include treatment,

(2) Reviewing the competence or qualifications of health care providers, evaluating practitioner and provide performance, health plan performance, conducting training programs in which students, trainees (e.g., HPTs) or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care provides, accreditation, certification, licensing or credentialing activities,

(3) Underwriting, enrollment, premium rating and other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance),

(4) Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs,

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies, and

(6) Business management and general administrative activities of the entity, including, but not limited to, management activities relating to implementation of and compliance with the HIPAA requirements; customer service, including the provision of data analyses for policy holders, plan sponsors or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor or customer; resolution of internal grievances; creating de-identified health information or a limited data set; and fundraising for the benefit of the covered entity.

v. **Health Care Provider.** A health care provider is an organization or entity, including its employees, or an individual who provides treatment as defined by the HIPAA Privacy Rule, such as a health care system, pharmacy and physician.

w. **Health Information.** Health Information is any information, including genetic information, whether oral or recorded in any form or medium, created or received by a health care provider, health plan, public health authority, employer, life insurers, school or university or health care clearinghouse or health plan that relates to the past, present or future physical, mental health or condition of an individual; the provision of health care to an individual; or payment for the provision of health care to an individual. Health information includes occupational health information as well information pertaining to examination, medical history, diagnosis and findings or treatment, including laboratory examinations, X-rays, microscopic slides, photographs and prescriptions.

x. **Health Oversight Activities.** Health oversight activities are activities authorized by law, including audits; civil, administrative or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative or criminal proceedings or actions;

or other activities necessary for appropriate oversight of: (1) The health care system; (2) Government benefit programs for which health information is relevant to beneficiary eligibility; (3) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or (4) Entities subject to civil rights laws for which health information is necessary for determining compliance.

y. **Health Record.** The health record is both the EHR and the paper record, where applicable. The health record is also known as the legal health record. The health record can be comprised of two divisions, the health record and the administrative record. The health record includes documentation of all types of health care service provided to an individual in any aspect of health care delivery. The term includes records of care in any health-related setting used by health care providers while providing patient care services, reviewing patient data or documenting their own observations, actions or instructions. The administrative record contains the administrative aspects involved in the care of a patient, including demographics, eligibility, billing, correspondence and other business-related information.

z. **Individual.** An individual is a person who is the subject of the individually identifiable information, including PHI, or their personal representative.

aa. **Individually Identifiable Information.** Individually identifiable information is any information pertaining to an individual that is retrieved by the individual's name or other unique identifier, as well as individually identifiable health information regardless of how it is retrieved. Individually identifiable information is a subset of personally identifiable information and is protected by the Privacy Act. ***NOTE:*** *Appendix C shows the relationship between the various data definitions, including individually identifiable information in relations to personally identifiable information.*

bb. **Individually Identifiable Health Information.** Individually identifiable health information 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 health or 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 individually identifiable health information to define information covered by the Privacy Act and the title 38 United States Code confidentiality statutes, in addition to HIPAA. Individually identifiable health information does not have to be retrieved by name or other unique identifier to be covered by this directive. Appendix C shows the relationship between the various data definitions.*

cc. **Infection with the Human Immunodeficiency Virus.** Infection with HIV is the presence of laboratory evidence for HIV. The term HIV has the same meaning as in 38 C.F.R. § 1.460.

dd. **Information Blocking.** Information blocking means a practice except as required by law or specified in rulemaking that is known by VHA, as a health care provider, to be unreasonable and likely to interfere with, prevent or materially discourage access, exchange or use of electronic PHI. It is not information blocking if VHA does not fulfill a request to access, exchange or disclose electronic PHI due to prohibition due to privacy under applicable Federal privacy laws and regulations or infeasibility of the request.

ee. **Law Enforcement Official.** A law enforcement official is an officer or employee of any agency or authority of the U.S., a State, a territory, a political subdivision of a State, or territory or an Indian tribe, who is empowered by law to conduct the following law enforcement activities:

(1) Investigate or conduct an official inquiry into a violation or potential violation of law, or

(2) Prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law.

ff. **Limited Data Set.** A limited data set is PHI from which certain specified direct identifiers of the individuals and their relatives, household members and employers have been removed. These identifiers include name, address (other than town or city, State or Zip code), phone number, fax number, email address, SSN, medical record number, health plan number, account number, certificate or license numbers, vehicle identification, device identifiers, web universal resource locators (URL), internet protocol (IP) address numbers, biometric identifiers and full-face photographic images. The two patient identifiers that can be used are dates and postal address information that is limited to town or city, State or Zip code. Thus, a limited data set is not de-identified information and it is covered by the HIPAA Privacy Rule. A limited data set may be used and disclosed for research, health care operations and public health purposes pursuant to a DUA. See 45 C.F.R. § 164.514(e)(2). ***NOTE:*** *Appendix C shows the relationship between the various data definitions.*

gg. **Logbook.** A logbook is a list containing information on multiple individuals with specific identifiers that is maintained over time for the purpose of tracking or review. ***NOTE:*** *Research records maintained by the investigator that span the entire lifecycle of the project, such as case report forms and subject regulatory files, are Federal records and do not constitute logbooks. Refer to the VHA RCS 10-1, Item 8300.6.*

hh. **Marketing.** Marketing is to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing excludes communications made to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by VHA in exchange for making the communication is reasonably related to VHA's cost of making the communication; for the following treatment and health care operations, except where VHA receives financial remuneration (i.e., direct or indirect payment from or on behalf of

a third party whose product or service is being described and does not include any payment for treatment of an individual) in exchange for making the communication:

(1) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers or settings of care to the individual,

(2) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits, or

(3) For case management or care coordination, contacting of individuals with information about treatment alternatives.

ii. **Next-of-kin.** For purposes of this directive, next-of-kin is a person such as a spouse, adult child, parent, adult sibling, grandparent or adult grandchild of the individual is not automatically a personal representative of the individual except that VHA recognizes a next-of-kin as a personal representative of a deceased individual.

jj. **Non-Identifiable Information.** Non-identifiable information is information from which all unique identifiers have been removed so that the information is no longer protected under the Privacy Act, 38 U.S.C. §§ 5701 or 7332. However, non-identifiable information has not necessarily been de-identified and may still be covered by the HIPAA Privacy Rule unless all 18 patient identifiers listed in the HIPAA Privacy Rule de-identification standards are removed. ***NOTE:*** *Appendix C shows the relationship between the various data definitions.*

kk. **Patient.** For purposes of this directive, a patient is a recipient of VA-authorized health care under title 38 United States Code, a sharing agreement or humanitarian auspices. This includes, but is not limited to, care in a: VA medical facility, nursing home care unit, community nursing home, domiciliary, outpatient clinic or readjustment counseling center.

ll. **Patient Identifiers.** Patient identifiers are the 18 data elements attributed to an individual under the HIPAA Privacy Rule that must be removed from health information for it to be de-identified and no longer covered by the HIPAA Privacy Rule. See Appendix A for more detail.

mm. **Payment.** Except as prohibited under 45 C.F.R. § 164.502(a)(5)(i), payment is an activity undertaken by a health plan to obtain premiums, to determine its responsibility for coverage or to provide reimbursement for the provision of health care including eligibility, enrollment and authorization for services. Payment includes activities undertaken by a health care provider to obtain reimbursement for the provision

of health care including pre-certification and utilization review. ***NOTE:*** *VHA is both a health plan and a health care provider.*

nn. **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 a POA, 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).

oo. **Personally Identifiable Information.** Personally identifiable information is 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 personally identifiable information elements includes but not limited to: name, SSN, 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". Personally identifiable information may not be protected by the Privacy Act as if it is not requires to be retrieved by name or unique identifier. Appendix C shows the relationship between the various data definitions.*

pp. **Personnel.** Personnel are officers and employees of VA; consulting and attending physicians; without compensation (WOC) workers; Intergovernmental Person Act (IPA) employees; contractors; others employed on a fee basis; HPTs; and volunteer workers, excluding patient volunteers, rendering uncompensated services, at the direction of VA staff. ***NOTE:*** *CWT patients are part of VHA Vocational and Rehabilitation Services program. They are not VHA personnel; they are patients receiving active treatment or therapy.*

qq. **Privacy Board.** Privacy Board is a term created by the HIPAA Privacy Rule to describe a board comprised of members with varying backgrounds and appropriate professional competencies, as necessary, to review the effect of a research protocol on an individual's privacy rights when an Institutional Review Board (IRB) does not.

rr. **Protected Health Information.** The HIPAA Privacy Rule defines PHI as 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 define information that is covered by HIPAA but unlike individually identifiable health information, 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. Appendix C shows the relationship between the various data definitions.*

ss. **Psychotherapy Notes.** Psychotherapy notes are notes recorded by a VA treating health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session (or a group,

joint or family counseling session) and that are separated from the rest of the individual's health record. Psychotherapy notes exclude counseling session times, modalities and frequencies of treatment, results of tests and any summary of diagnosis, status, treatment plan or progress to date. Psychotherapy notes are the personal session notes of the mental health professional for use in composing progress notes for the official VHA health record (see 45 C.F.R. § 164.501). Psychotherapy notes may not be used or disclosed by the mental health professional without the prior written authorization of the individual to whom the notes pertain. Psychotherapy notes within VHA are not considered PHI as they are not Federal agency records owned by VHA.

tt. **Public Health.** Public health is the science of protecting and improving the health of people and their communities and is concerned with protecting the health of entire populations. ***NOTE:*** *Public health performed by an entity other than a public health authority may include research. See VHA Directive 1200.05(3) for guidance.*

uu. **Public Health Authority.** A public health authority is an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from, or contract with, such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate (see 45 C.F.R. § 164.501).

vv. **Record.** For purposes of this policy, a record is any item, collection or grouping of information about an individual that is VHA-maintained, including, but not limited to: education, financial transactions, medical history, treatment and criminal or employment history that contains the name, or an identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph. Records include information that is stored in any medium including paper; film and electronic media; and computers, minicomputers and personal computers or word processors. ***NOTE:*** *Tissue samples or any other physical items, such as clothing, are not considered a record.*

ww. **Required by Law.** For purposes of this policy, required by law means a mandate contained in Federal, State, local or tribal law and enforceable under the law that compels an entity to collect, create, use or disclose PHI. This includes, but is not limited to, disclosures under FOIA, court orders, court-ordered warrants and summonses issued by a governmental or tribal inspector general.

xx. **Routine Use.** A routine use is a statement of Privacy Act discretionary authority, published in the Federal Register in advance of a disclosure, which permits VHA to disclose information or records from a Privacy Act System of Records to a person or entity outside of VA without the prior signed-written authorization of the individual who is the subject of the information. A routine use permits the:

(1) Release of PHI only when disclosure is also authorized by other applicable legal authorities, including the HIPAA Privacy Rule, and

(2) Release of drug or alcohol abuse, HIV or sickle cell anemia medical information only when the disclosure is also authorized by 38 U.S.C. § 7332.

yy. **Sensitive Personal Information.** Sensitive personal information (SPI), with respect to an individual, is any information about the individual maintained by an agency, including the following: (1) education, financial transactions, medical history and criminal or employment history; and (2) information that can be used to distinguish or trace the individual's identity, including name, SSN, Integrated Control Number (ICN), date and place of birth, mother's maiden name or biometric records. SPI is a subset of VA Sensitive Information/Data. See 38 U.S.C. § 5727. ***NOTE:*** *The term "Sensitive Personal Information" is synonymous and interchangeable with "Personally Identifiable Information."*

zz. **Subcontractor.** A subcontractor is a person to whom a Business Associate delegates a function, activity or service, other than in the capacity of a member of the workforce of such Business Associate.

aaa. **Subpoena.** For purposes of this directive and the Privacy Act, a subpoena is a document issued by, or under the auspices of, a court to cause an individual to appear and give testimony before a court of law. A subpoena cannot require VHA to disclose Privacy Act-protected records, unless the subpoena is signed by a judge making it a court order.

bbb. **Subpoena Duces Tecum.** For purposes of this directive and the Privacy Act, a subpoena duces tecum is a document issued by, or under, the auspices of a court that requires an individual to produce documents, records, papers or other evidence to be brought to a judicial court for inspection. A subpoena duces tecum is not sufficient authority to authorize the disclosure of Privacy Act-protected records, unless the subpoena is signed by the judge making it a court order.

ccc. **Surrogate Decision Maker (Surrogate).** A surrogate is an individual(s) authorized to make health care decisions on behalf of a patient who lacks decision-making capacity. The authorized surrogate in hierarchical order may be the health care agent, the legal guardian, spouse, child, parent, sibling, grandparent or grandchild or a close friend.

ddd. **System of Records.** A System of Records is a group of Privacy Act-covered records that contains personal information about an individual from which information is retrieved by the name of the individual or by some identifying number, symbol or other identifying particular assigned to an individual. A notice defining a System of Records must be published in the Federal Register. A System of Records is also a designated record set.

eee. **System Manager.** The System Manager is the VHA official or program office assigned the responsibility for a Privacy Act-covered System of Records as identified in the system description that is published in the Federal Register in accordance with VA

Handbook 6300.5. The VA health care facility official with the program assignment is responsible for the maintenance of the records at the facility.

fff. **Treatment.** For purposes of this directive and as defined by HIPAA, treatment is the provision, coordination or management of heath care or related services by one or more health care providers. This includes the coordination of health care by a health care provider with a third-party consultation between health providers relating to a patient and the referral of a patient for health care from one health care provider to another.

ggg. **Unique Identifier.** A unique identifier is an individual's name, address, SSN, or some other identifying number, symbol, or code assigned only to that individual (e.g., medical record number and claim number). If these identifiers are removed, then the information is no longer personally identifiable information and is no longer covered by the Privacy Act or 38 U.S.C. §§ 5701 and 7332. However, if the information was originally individually identifiable health information, then it would still be covered by the HIPAA Privacy Rule unless all 18 patient identifiers listed in the de-identification standard have been removed. ***NOTE:*** *OGC has indicated that the first initial of an individual's last name and last four of their SSN (e.g., A2222) is not a unique identifier; therefore, inclusion of this number by itself does not make the information identifiable or sensitive.*

hhh. **Use.** Use means, with respect to personally identifiable information, the accessing, viewing, sharing, employment, application, utilization, examination or analysis of such information by and within VHA.

iii. **VA Health Care Facility.** For the purpose of this directive, VA health care facility means each office and operation under the jurisdiction of VHA, including but not limited to VHA program offices, VISN offices, VA medical centers, VA Health Care Systems, Community Based Outpatient Clinics (CBOCs), Readjustment Counseling Centers (Vet Centers) and Research Centers of Innovation (COIN). ***NOTE:*** *The use of the term "facility" in this directive is synonymous with this definition.*

jjj. **VA Medical Facility.** For the purpose of this directive, VA medical facility means VA medical centers, VA health care systems, CBOCs and VA Community Living Centers that provide inpatient, long-term care and ambulatory care services to patients within a VISN.

kkk. **VA Treating Health Care Provider.** VA treating health care provider includes any individual who is licensed to provide care such as physicians, nurses and therapists, and who is providing care and treatment to a patient.

lll. **VHA Employee.** For purposes of this directive, VHA employee means a VA employee in a position, whether under title 5 or title 38 of the United States Code, within VHA under the jurisdiction and authority of the programs administered by the Under Secretary of Health.

42. REFERENCES

a. P.L. 104-191, Health Insurance Portability and Accountability Act of 1996 (HIPAA).

b. P.L. 106-229, Electronic Signatures in Global and National Commerce Act.

c. P.L. 114-255, Title IV, 21st Century Cures Act.

d. P.L. 115-182, VA Mission Act of 2018.

e. P.L. 115-424, Victims of Child Abuse Act Reauthorization Act of 2018.

f. 5 U.S.C. §§ 552, 552a and 7114(b)(4).

g. 10 U.S.C. part 2.

h. 21 U.S.C. § 880.

i. 34 U.S.C. § 20341.

j. 38 U.S.C. §§ 1.511(c), 5302, 5701, 5705, 7307, 7332 and 8111A.

k. 42 U.S.C. § 405 Note, Social Security Number Fraud Prevention Act of 2017.

l. 44 U.S.C. § 3501-3521.

m. 5 C.F.R. part 1320.

n. 38 C.F.R. §§ 0.605, 1.460-1.582, 1.900-1.970, 5723(f) and 17.500-17.511.

o. 45 C.F.R. parts 16, 160 and 164.

p. VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management, dated September 2, 2014.

q. VA Directive 6213, Freedom of Information Act (FOIA), dated September 15, 2021.

r. VA Directive 6310, Forms, Collections of Information, and Reports Management, dated December 1, 2001.

s. VA Directive 6371, Destruction of Temporary Paper Records, dated April 8, 2014.

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

u. VA Directive 6502, VA Enterprise Privacy Program, dated May 5, 2008.

v. VA Directive 6509, Duties of Privacy Officers, dated July 30, 2015.

w. VA Directive 6511, Presentations Displaying Personally Identifiable Information, dated January 7, 2011.

x. VA Handbook 6300.1, Records Management Procedures, dated March 24, 2010.

y. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, dated August 19, 2013.

z. VA Handbook 6300.5, Procedures for Establishing and Maintaining Privacy Act Systems of Records, dated August 3, 2017.

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

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

cc. VA Handbook 6500.6, Contract Security, dated March 12, 2010.

dd. VHA Directive 1078, Privacy of Persons Regarding Photographs Digital Images and Video or Audio Recordings, dated November 29, 2021.

ee. VHA Directive 1080.01(1), Data Use Agreements, dated January 19, 2021.

ff. VHA Directive 1100.21(1), Privileging, dated March 2, 2023.

gg. VHA Directive 1131(5), Management of Infectious Disease and Infection Prevention and Control Programs, dated November 7, 2017.

hh. VHA Directive 1134(2), Provision of Medical Statements and Completion of Forms by VA Health Care Providers, dated November 28, 2016.

ii. VHA Directive 1192.01, Seasonal Influenza Vaccination Program for VHA Health Care Personnel, dated August 10, 2020.

jj. VHA Directive 1199(2), Reporting Cases of Abuse and Neglect, dated November 28, 2017.

kk. VHA Directive 1200.01(1), Research and Development Committee, dated January 24, 2019.

ll. VHA Directive 1200.05(3), Requirements for the Protection of Human Subjects in Research, dated January 7, 2019.

mm. VHA Directive 1206, Use of a Cooperative Research and Development Agreement (CRADA), dated June 19, 2018.

nn. VHA Directive 1412(1), Department of Veterans Affairs Cancer Registry System, dated May 29, 2019.

oo. VHA Directive 1500(3), Readjustment Counseling Service, dated January 26, 2021.

pp. VHA Directive 1605, VHA Privacy Program, dated September 1, 2017.

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

rr. VHA Directive 1605.03(2), Privacy Compliance and Accountability Program, dated September 19, 2019.

ss. VHA Directive 1605.05, Business Associate Agreements, dated November 17, 2020.

tt. VHA Directive 1615, Mandated Utilization of Release of Information (ROI) Plus Software, dated March 23, 2022.

uu. VHA Directive 1906, Data Quality Requirements for Health Care Identity Management and Master Veteran Index Functions, dated April 10, 2020.

vv. VHA Directive 1907.01, VHA Health Information Management and Health Records, dated April 5, 2021.

ww. VHA Directive 1935, VHA Freedom of Information Act Program, dated February 5, 2018.

xx. VHA Directive 2010-052, Management of Wandering and Missing Patients, dated December 3, 2010.

yy. VHA Directive 6370, Compensation and Pension (C&P) Examination Report Release of Information, dated August 22, 2019.

zz. VHA Handbook 1000.02, VHA Fugitive Felon Program, dated February 23, 2012.

aaa. VHA Handbook 1004.02, Advance Care Planning and Management of Advance Directives, dated December 24, 2013.

bbb. VHA Handbook 1100.17, National Practitioner Data Bank (NPDB) Reports, dated December 28, 2009.

ccc. VHA Handbook 1200.12, Use of Data and Data Repositories in VHA Research, dated March 9, 2009.

ddd. VHA Handbook 1605.04, Notice of Privacy Practices, dated October 7, 2015.

eee. VA Form 10-0137, VA Advance Directive: Durable Power of Attorney for Health Care and Living Will.

fff. VA Form 10-0137A, What You Should Know About Advance Directives.

ggg. VA Form 10-250, VHA Research Protocol Privacy Review Checklist.

hhh. VA Form 10-3203a, Informed Consent and Authorization for Third Parties to Produce or Record Statements, Photographs, Digital Images, or Video or Audio Recordings.

iii. VA Form 10-0493, Authorization for Use and Release of Individually Identifiable Health Information Collected for Veterans Health Administration (VHA) Research.

jjj. VA Form 10-5345, Request for and Authorization to Release Health Information.

kkk. VA Form 10-5345a, Individuals' Request for a Copy of Their Own Health Information.

lll. VA Form 10-9050, HCP Influenza Vaccination Form.

mmm. VA Form 10-10163 - Request for and Permission to Participate in Sharing Protected Health Information through Health Information Exchanges.

nnn. VA Form 10-10164, Opt-Out of Sharing Protected Health Information Through Health Information Exchanges.

ooo. VA Form 10-10EZ, Instructions For Completing Enrollment Application for Health Benefits.

ppp. VA Form 21-22, Appointment of Veterans Service Organization as Claimant's Representative.

qqq. VA Form 21-22a, Appointment of Individual as Claimant's Representative.

rrr. VA Form 4763, Power of Attorney and Assignment.

sss. VA Medical Center Privacy Policy Template. https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/templates.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

ttt. VHA Privacy Office Guidebooks, Fact Sheets and Practice Briefs. https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/FactSheets.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

uuu. VHA CBO Procedure Guide, Federal Workers' Compensation Reasonable Charges and Billing. https://vaww.vrm.km.va.gov/system/templates/selfservice/va_kanew/help/agent/locale/en-US/portal/554400000001031/content/554400000050620/Section-H-Federal-Workers-Compensation-Reasonable-Charges-and-Billing. ***NOTE:*** *This is an internal VA website that is not available to the public.*

vvv. VHA Systems of Records notices: https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/SystemofRecords.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

www. VHA Facility Directory Opt-Out in the Community Care Procedure Guide. https://vaww.vrm.km.va.gov/system/templates/selfservice/va_kanew/help/agent/locale/en-US/portal/554400000001031/content/554400000050778/Section-E-Patient-Counseling?query=opt%20out. ***NOTE:*** *This is an internal VA website that is not available to the public.*

xxx. ROI Plus Administrative Manual. https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/roi.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

yyy. Business Associate Agreements. http://vaww.vhadataportal.med.va.gov/PolicyAdmin/BusinessAssociateAgreements.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

zzz. Department of Defense 6025.18, Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs, dated March 13, 2019.

aaaa. Drug Enforcement Agency Form 82, Notice of Consent to Inspection.

bbbb. OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.

cccc. Social Security Administration Form SSA-827, Authorization to Disclose Information to the Social Security Administration.

DE-IDENTIFICATION OF DATA

1. INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION

Individually identifiable health information 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 Health Insurance Portability and Accountability Act (HIPAA)-covered entity, such as the Veterans Health Administration (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.

2. DE-IDENTIFICATION

VHA considers health information to be de-identified (not individually identifiable) only if the steps outlined in paragraphs 2.a. or 2.b. of this appendix are met for the releases specified:

a. **Expert Determination.** A qualified biostatistician (an individual with a master's or Ph.D. degree related to statistics) who has extensive background in statistics, mathematics, science and appropriate knowledge of, and experience with, generally accepted statistical and scientific principles and methods for de-identification applying generally accepted statistical and scientific principles and methods:

(1) Determines that the risk that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information is very small; and

(2) Documents the methods and results of the analysis that justify such determination.

NOTE: *Genetic information must only be de-identified using expert determination.*

b. **Safe Harbor.** VHA does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information and the following identifiers of the individual or of relatives, employers or household members of the individual are removed:

(1) Names.

(2) All geographic subdivisions smaller than a State, including street address, city, county, precinct, Zip code and their equivalent geocodes, except for the initial three digits of a Zip code if, according to the current publicly available data from the Bureau of the Census:

(a) The geographic unit formed by combining all Zip codes with the same three initial digits contains more than 20,000 people; and

(b) The initial three digits of a Zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

NOTE: *VHA considers the de-identification standard of the HIPAA Privacy Rule for protecting addresses as acceptable under 38 U.S.C. § 5701.*

(3) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.

(4) Telephone numbers.

(5) Fax numbers.

(6) Electronic mail addresses.

(7) Social Security Numbers (SSNs).

(8) Medical record numbers.

(9) Health plan beneficiary numbers.

(10) Account numbers.

(11) Certificate or license numbers.

(12) Vehicle identifiers and serial numbers, including license plate numbers.

(13) Device identifiers and serial numbers.

(14) Web Universal Resource Locators (URLs).

(15) Internet Protocol (IP) address numbers.

(16) Biometric identifiers, including finger and voice prints.

(17) Full-face photographic images and any comparable images.

(18) Any other unique identifying number, characteristic or code, except as permitted by paragraph 3 of this appendix. A diagnosis or procedure code is not a unique identifying code.

NOTE: *Scrambling of names and SSNs is not considered de-identifying health information for the purposes of this directive.*

3. RE-IDENTIFICATION CODE

a. VHA may assign a code, or other means of record identification, in order to allow information de-identified under paragraph 2.b. of this appendix, or to be re-identified by VHA, provided that:

(1) The code or other means of record identification is not derived from, or related to, information about the individual and that the code is not otherwise capable of being translated so as to identify the individual. ***NOTE:*** *While first initial of last name and last four digits of the SSN is not a unique identifier for a single individual, it would meet the definition of a re-identification code that violates this provision when included in a data set containing records on multiple individuals*;

(2) The code, or other means of re-identification, is not used or disclosed by VHA for any other purpose; and

(3) VHA does not disclose the mechanism (e.g., algorithm or other tool) for re-identification.

b. The code or other means of record identification is not considered one of the identifiers that must be excluded for de-identification. ***NOTE:*** *When disclosing de-identified data to non-Department of Veterans Affairs (VA) entities this code needs to be removed.*

4. RANDOM IDENTIFIER

VHA may assign a random number or code to de-identified data in order to segregate one record from another. The number or code must be created through random processes and cannot be derived from, or related to, information about the individual, such as SSN. This random number or code is not a re-identification code and can be disclosed when disclosing the de-identified data set to non-VA entities.

NON-VHA SYSTEMS OF RECORDS

Copies of Department of Veterans Affairs (VA) and Government-wide Systems of Records notices listed in the following table can be obtained from the Government Printing Office (GPO) Privacy Act Issuances Website at: http://www.gpo.gov/fdsys/browse/collection.action?collectionCode=PAI.

System Name	*System Number*	*System Manager*	*Responsible Office*	*Types of Records*
Applicants for Employment under Title 38-VA	02VA135	05	Office of Personnel and Labor Relations	Title 38 Employment
Employee Medical Folder System Records Title38-VA	08VA05	05	Office of Personnel and Labor Relations	Title 38 Employment
Employee Unfair Labor Practice Charges and Complaints, Negotiated Agreement Grievances and Arbitrations-VA	09VA05	05	Office of Personnel and Labor Relations	Employment
VA Supervised Fiduciary/Beneficiary and General Investigative Records-VA	37VA27	27	Veterans Assistance Services	Fiduciary Records
Compensation, Pension, Education and Vocational Rehabilitation and Employment Records-VA	58VA21/ 22/28	21/22	Veterans Assistance Services	Compensation. Pension, Rehabilitation Records

System Name	*System Number*	*System Manager*	*Responsible Office*	*Types of Records*
Police and Security Records-VA	103VA07B	07B	VA Police and Security Service	Law Enforcement
General Personnel Records	Office of Personnel Management (OPM), i.e., Government (GOVT)-1	OPM	Office of Personnel and Labor Relations	Title 5 Employment
Employee Performance File System Records	OPM/ GOVT-2	OPM	Office of Personnel and Labor Relations	Title 5 Employment
Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions and Termination of Probationers	OPM/ GOVT-3	OPM	Office of Personnel and Labor Relations	Title 5 Employment
Recruiting, Examining and Placement Records	OPM/ GOVT-5	OPM	Office of Personnel and Labor Relations	Title 5 Employment
Personnel Research and Test Validation Records	OPM/ GOVT-6	OPM	Office of Personnel and Labor Relations	Title 5 Employment

System Name	*System Number*	*System Manager*	*Responsible Office*	*Types of Records*
File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals and Fair Labor Standard Act (FLSA) Claims and Complaints	OPM/ GOVT-9	OPM	Office of Personnel and Labor Relations	Title 5 Employment
Employee Medical File System Records-VA	OPM/ GOVT-10	OPM	Office of Personnel and Labor Relations	Title 5 Employment

DATA RELATIONSHIPS

The Veterans Health Administration (VHA) uses many different terms to describe information or data maintained by the administration as a health plan and health care provider. The below data terms are listed in order of broadest to narrowest set of information for VHA. When a broader data term is used within this directive indicating permissible use and disclosure of the information, all subsequently listed data terms are included unless explicitly excluded.

a. **Sensitive Personal Information/Personally Identifiable Information.** Personally identifiable information is the broadest category of identifiable information, including information that may not be protected by the Privacy Act or Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

b. **Individually Identifiable Information.** Subset of personally identifiable information that is always protected by the Privacy Act and does not have to be health information.

c. **Individually Identifiable Health Information.** Health information that is a subset of III protected by the HIPAA Privacy Rule, Privacy Act, 38 U.S.C. § 5701 and when applicable 38 U.S.C. § 7332.

d. **Protected Health Information.** Individually identifiable health information transmitted or maintained in any form or medium by VHA, as a health plan or health care provider, that has not been de-identified in accordance with the HIPAA Privacy Rule.

e. **38 U.S.C. § 7332-protected information.** Subset of individually identifiable health information that is health information related to the diagnosis of HIV or sickle cell anemia, and the treatment of drug abuse, alcoholism or alcohol abuse as defined by 38 U.S.C. § 7332.

f. **Non-identifiable Information.** Subset of personally identifiable information from which all unique identifiers have been removed so that the information is no longer protected under the Privacy Act, 38 U.S.C. §§ 5701 or 7332. Non-identifiable information that is health information is still protected under the HIPAA Privacy Rule as it is not de-identified.

g. **Limited Data Set.** A subset of PHI from which certain specified direct identifiers of the individuals and their relatives, household members and employers have been removed, but is still protected under the HIPAA Privacy Rule as it is not de-identified.

h. **De-identified Data.** Health information that is presumed not to identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual as the health information has been de-identified in accordance with the HIPAA Privacy Rule. De-identified data is no longer

covered by the Privacy Act, 38 U.S.C. §§ 5701 or 7332, the HIPAA Privacy Rule and is no longer considered personally identifiable information. FOIA may apply to requests for the disclosure of de-identified data.