PRIVACY AND RELEASE OF INFORMATION

1. REASON FOR ISSUE: This Veterans Health Administration (VHA) directive provides revised instructions on compliance with the Privacy Act and the release of information from drug and alcohol abuse, infection with the human immunodeficiency virus, and sickle cell anemia health records.

2. SUMMARY OF MAJOR CHANGES: This directive revises, consolidates, and updates procedures involving privacy and the release of information. This directive also establishes VHA procedures regarding compliance with the provisions of the Standards of Privacy of Individually-Identifiable Health Information, 45 Code of Federal Regulations (CFR) Parts 160 and 164 (the HIPAA Privacy Rule). This directive removes provisions addressing compliance with the Freedom of Information Act (FOIA), which are addressed in VA Handbook 6300.3.

3. RELATED ISSUES: VA Handbook 6300.3 through VA Handbook 6300.7 as well as VHA Handbooks included in the 1605 series.

4. RESPONSIBLE OFFICE: The VHA Office of Informatics and Information Governance , Information Access and Privacy (10P2C), is responsible for the content of this directive. Questions may be referred to the VHA Privacy Officer at 704-245-2492.

5. RESCISSION: VHA Handbook 1605.1, dated May 17, 2006, is rescinded.

6. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last working day of August 2021.

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

DISTRIBUTION: Emailed to the VHA Publications Distribution List on 09/02/2016.

CONTENTS

PRIVACY AND RELEASE OF INFORMATION

PRIVACY AND RELEASE OF INFORMATION

1. PURPOSE

This Veterans Health Administration (VHA) directive establishes the VHA privacy practices procedures for the use and disclosure of individually-identifiable information, and individual privacy rights related to VHA health care data. This directive defines the responsibilities and requirements for VHA compliance with all Federal confidentiality and privacy laws and regulations. When using or disclosing VHA information, all applicable laws and regulations must be reviewed and applied simultaneously to the use or disclosure. This directive should 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, 7332, 38 CFR 1.460-1.582, 17.500-17.511, and 45 CFR parts 160 and 164.

2. BACKGROUND

a. VHA, as a component of a government agency and as a health plan and health care provider, must comply with all applicable privacy and confidentiality statutes and regulations. The most commonly encountered statutes and sets of regulations are identified in paragraph 2.b. and addressed by this directive. Questions concerning other confidentiality and privacy legal requirements not covered in this directive should be addressed to the VA Office of General Counsel or Regional Counsel. Generally, the same privacy rules apply across the Department of Veterans Affairs (VA). However, regulations promulgated by the Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 impose additional requirements on VHA's privacy practices for protected health information. The HIPAA regulations impose specific requirements for VHA to act, in certain circumstances, as a separate entity from the rest of VA. This directive provides the guidance for 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 release of information from VHA records are:

(1) **The Freedom of Information Act (FOIA).** Title 5 United States Code (U.S.C.) 552, implemented by Title 38 Code of Federal Regulations (CFR), Sections 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 one or more of nine exemptions apply to the records (see 5 U.S.C. 552(b)(1)-(b)(9) and 38 CFR 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 are 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 CFR

1.550-1.562, and VA Handbook 6300.3, Procedures for Implementing the Freedom of Information Act.

(2) **The Privacy Act, 5 U.S.C. 552a, implemented by VA at 38 CFR 1.575-1.582.** Generally, the Privacy Act provides for the confidentiality of individually-identifiable information about living individuals retrieved by name or other 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-identifiable and identifiable information must be maintained in a manner that precludes unwarranted intrusion upon individual privacy. Information is collected directly from the subject 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 CFR Section 1.500-1.527.** Section 5701 of 38 U.S.C. 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. Title 38 CFR Sections 1.500-1.527, are not to be used in releasing information from patient health records when in conflict with The Privacy Act, Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, HIV and Sickle Cell Anemia Medical Records, or HIPAA.

(4) **Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Health Records, 38 U.S.C. 7332, implemented by 38 CFR Section 1.460-1.496.** Section 7332 of 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 and the testing and treatment of sickle cell anemia or HIV infection, including negative or positive test results. 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 for each of the following circumstances:

(a) To medical personnel to the extent to meet a bona fide medical emergency;

(b) To qualified personnel for conducting scientific research, management audits, financial audits or program evaluations;

(c) To a public health authority charged under federal or state law with the protection of public health pursuant to a standing written request;

(d) To a court of competent jurisdiction pursuant to a Court Order;

(e) To the Department of Defense (DoD);

(f) To a uninformed spouse or sexual partner of HIV-positive patient;

(g) To a State Prescription Drug Monitoring Program (SPDMP);

(h) To the next of kin to obtain survivorship benefits; or

(i) To the patient's surrogate under the conditions specified in paragraph 24.e.

(5) **HIPAA (Public Law 104-191), implemented by 45 CFR 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.

(6) **Confidentiality of Medical Quality Assurance Review Records, 38 U.S.C. 5705, implemented by 38 CFR Section 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.

c. When following VHA policies, all six statutes will be applied simultaneously. VHA 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 VHA health care data and in the exercise of the greatest rights of the individual. For example, when an individual 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 (see Appendix A).*

d. **Compliance with Federal Law, Regulation, and VHA Policy.**

(1) All VHA employees must comply with all Federal laws and regulations, VA regulations and policies, and VHA policies.

(2) All employees must conduct themselves in accordance with the rules of conduct concerning the disclosure or misuse of information. Employees are required to annually sign the VA National Rules of Behavior per VA Handbook 6500, Appendix D.

(3) All VHA health care facilities must create facility procedures using the VHA facility Policy and Procedure template which is consistent with procedures and policies contained in this directive. This template can be found at http://vaww.vhaco.va.gov/privacy/templates.htm. This policy must be posted and available to all employees (e.g., posted on the facility's internal web site).

(4) All VA employees who have access to VHA 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, and/or facility or office policies and procedures regarding privacy, and as otherwise directed in paragraph 38.g. of this directive, Training of Personnel.

(5) VA may not collect or maintain information about individuals that is retrieved by a personal identifier until proper notifications are given to Congress and the Office of Management and Budget (OMB), and a notice is published in the *Federal Register* as required by the Privacy Act.

e. **Use of Information.**

(1) All VHA employees may use information contained in VHA records when they need the records in the performance of their official job duties for treatment, payment, and/or health care operations (TPO) 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 a friend or out of curiosity is strictly prohibited and is a privacy violation. Appropriate disciplinary action may be taken by the supervisor with guidance from Human Resources.

(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 Handbook 1605.02, Minimum Necessary Standard for Protected Health Information.

(3) Where VHA has determined that it is legally permissible to provide access to information or data protected by one or more of the applicable confidentiality or privacy provisions, VHA may do so only after complying with the relevant legal requirements.

(4) Sharing of individually-identifiable information for official VA approved research may require the completion of a Data Use Agreement (DUA) (see paragraph 13, Research; VHA Handbook 1080.01, Data Use Agreement and VHA Handbook 1200.12, Use of Data and Data Repositories in VHA Research).

(5) VHA may use a limited data set for the purpose of research, public health, or health care operations without obtaining a HIPAA authorization or waiver of HIPAA authorization. VHA may use individually-identifiable 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, but a limited data set may contain dates, state, city; and full 5 or 9-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 CFR Part 16, and this directive.

(8) The Office of General Counsel Advisory Opinion (VAOPGCADV B-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.

f. **Disclosure of Information.**

NOTE: *Throughout this directive, various situations are described in which individually-identifiable information may be disclosed. Because disclosure is discretionary, individually-identifiable information should 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 should be referred to the facility Privacy Officer or the VHA Privacy Officer in advance of the disclosure.*

(1) When VHA discloses individually-identifiable information pursuant to legal authority other than a signed, written authorization, the disclosing VHA official shall notify the recipient, preferably in writing, that the information disclosed is confidential and the information must be handled with appropriate sensitivity.

(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.

(3) Individually-identifiable information from VHA records can 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, Appendix A).

(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, and testing or treatment for HIV has special protection under 38 U.S.C. 7332. The information can be disclosed only as authorized by 38 U.S.C. 7332 and implementing VA regulations at 38 CFR 1.460–1.496.

(5) When disclosing individually-identifiable information with 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. Refer to VHA Handbook 1080.01, Data Use Agreements for detailed guidance.

(6) **Limited Data Sets.** VHA may disclose a limited data set for research and public health purposes and health care operations pursuant to a DUA or Memorandum of Understanding (MOU). See VHA Handbook 1080.01, Data Use Agreements.

g. **Safeguards.**

(1) VHA, including each health care facility, must ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of individually-identifiable information and records, including protected health information (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 a VA employee to:

(a) 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;

(b) Secure and safeguard all protected health information (PHI) by locking PHI in a file cabinet or desk drawer. PHI should not be left unattended per compliance with VA Handbook 6500;

(c) Destroy all documents containing PHI when no longer needed in accordance with VA Directive 6371, Destruction of Temporary Paper Records, and all applicable records control schedules;

(d) Comply with the requirements contained in the VA National Rules of Behavior found in VA Handbook 6500, Appendix D.

(2) Each VHA health care 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 should:

(e) Speak quietly when discussing a patient's condition with family members in a waiting room, telephone, or other public areas;

(f) Speak quietly to the patient when you are in an open area (e.g., emergency room or multiple bed ward); and

(g) Avoid speaking about patients' PHI in public hallways and elevators. Signs regarding principles of auditory privacy should be posted in public hallways and elevators to remind employees and others to protect patient confidentiality.

NOTE: *Facilities do not have to build private, soundproof rooms or alter existing space to prevent overheard conversations about a patient's condition. The HIPAA Privacy Rule simply requires that facilities provide reasonable safeguards to protect confidential information, such as using curtains, screens, white noise or similar barriers. If a 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.*

(3) Use of facsimile (fax) or email to disclose individually-identifiable information must strictly adhere to VA Handbook 6500, Information Security Program; VHA Handbook 1907.01, Health Information Management and Health Records; and this directive.

(4) No personal copies of VHA records can be maintained by VHA employees nor should VHA employee access their own records.

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

(6) All VHA employees who need to remove and/or transport individually-identifiable information in the performance of their official job duties must have prior written approval from their respective VA supervisor and Information Security Officer (ISO) before individually-identifiable information can be removed from VHA.

h. **Sale of Protected Health Information.**

(1) VHA may not, and does not, sell protected health information. VHA business associates may not sell protected health information received from VHA.

(2) Except as otherwise described in paragraph 2.h.(3) below, the sale of protected health information is a disclosure of protected health information 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 protected health information in exchange for the protected health information.

(3) The following disclosures of protected health information are not considered a sale of protected health information:

(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 protected health information 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; and

(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 protected health information for such purpose, or a fee otherwise expressly permitted by other law, such a FOIA fees.

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

3. 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 VA. This is not the same as the Sensitive Patient Access Report (SPAR).

c. **Alcohol Abuse.** Alcohol abuse is the use of an alcoholic beverage that impairs the physical, mental, emotional, or social well-being of the user.

d. **Amendment.** An amendment is the authorized alteration of health information by modification, correction, addition or deletion.

e. **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.

f. **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 CFR part 17.

g. **Close Friend.** A close friend is any person eighteen 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.

h. **Compensated Work Therapy Workers.** A compensated work therapy worker (CWT) 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 individually-identifiable information. VHA may not disclose or release any protected health information to a CWT Worker without the signed written authorization of the individual to whom the information pertains.

i. **Contractor.** A contractor means a person who provides services to VA such as data processing, dosage preparation, laboratory analyses or medical or other professional services. Each contractor shall be required to enter into a written agreement subjecting such contractor to the provisions of 38 CFR 1.460 through 1.499, 38 U.S.C. 5701 and 7332, and 5 U.S.C. 552a and 38 CFR 1.576(g).

j. **Court Leave.** For the purpose of this directive, court leave is the authorized absence from official duty of an employee, without charge to leave or loss of salary, to present records in court or to appear as a witness in the employee's official capacity.

k. **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.

l. **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.

m. **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 System of Records.

n. **Diagnosis.** Diagnosis is the identification of a disease, condition, situation, or problem based on the systematic analysis of signs and symptoms.

o. **Disclosure.** Disclosure means a communication of patient identifying information, the affirmative verification of another person's communication of patient identifying information, or the communication of any information from the record of a patient who has been identified.

p. **Drug Abuse.** Drug abuse means the use of a psychoactive substance for other than medicinal purposes which impairs the physical, mental, emotional, or social well-being of the user

q. **Extramural Research.** Extramural research as defined in VHA Directive 1200 is research performed by investigators not in the employ of VA, but who may be under contract with VA. For purposes of this directive, the privacy requirements for disclosing information to outside entities under contract with VA is covered under Intramural Research when the disclosure is necessary for the entity to fulfill the terms of the contract.

r. **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.

s. **Financial Remuneration.** Financial remuneration means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

t. **Fiduciary.** Fiduciary means 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 for the use and benefit of a minor, incompetent, or other beneficiary.

u. **Fundraising.** Fundraising is an organized activity or instance of soliciting money or pledges, such as for charitable organizations or political campaigns.

v. **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.

w. **Genetic Services.** Genetic services means genetic tests, genetic counseling (including obtaining, interpreting, or assessing genetic information), or genetic education.

x. **Genetic Test.** A genetic test means 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.

y. **Genetic Information Nondiscrimination Act of 2008.** Genetic Information Nondiscrimination Act of 2008 (GINA) gives individuals new privacy and nondiscrimination rights with respect to the use of genetic information in health insurance decisions and employment. VHA, as a health plan and health care provider, does not perform underwriting.

z. **Health care Operations.** Health care operations mean 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 CFR 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 professionals, evaluating practitioner and provide performance, health plan performance, conducting training programs in which students, trainees, 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 professionals, 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 protected health information 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.

aa. **Health care Provider.** For the purpose of this directive, the term health care provider includes an individual who is licensed to provide care such as physicians, nurses, and therapists.

bb. **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 information pertaining to examination, medical history, diagnosis, and findings or treatment, including laboratory examinations, X-rays, microscopic slides, photographs, and prescriptions, etc.

cc. **Health Record.** The health record consists of both the electronic health record 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 professionals 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.

dd. **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 (PII) and is protected by the Privacy Act.

ee. **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 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 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.*

ff. **Infection with the Human Immunodeficiency Virus.** Infection with Human Immunodeficiency Virus (HIV) is the presence of laboratory evidence for HIV. For the purposes of this directive, the term HIV has the same meaning as in 38 CFR § 1.460.

gg. **Intramural Research.** Intramural research is research performed by VA employees or appointees (including those serving without compensation) at VA facilities and approved off-site locations.

hh. **Law Enforcement Official.** A law enforcement official is an officer or employee of any agency or authority of the United States (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.

ii. **Legal Guardian.** 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.

jj. **Limited Data Set.** A limited data set is protected health information 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, Social Security Number (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 Data Use Agreement. See 45 CFR 164.514(e)(2).

kk. **Marketing.** Marketing means 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 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.

ll. **Medical Emergency.** A medical emergency is a condition that poses an immediate threat to the health or life of a person that requires immediate medical intervention.

mm. **Next-of-kin.** For purposes of this directive 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.

nn. **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.

oo. **Patient.** For purposes of this directive, a patient is a recipient of VA-authorized health care under 38 U.S.C. Veterans' Benefits. This includes, but is not limited to, care in a: VA medical center, nursing home care unit, community nursing home, domiciliary, outpatient clinic or readjustment counseling center.

pp. **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, De-Identification of Data, for more detail.

qq. **Payment.** Except as prohibited under 45 CFR 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.*

rr. **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 power of attorney, legal guardianship of the individual, appointment as executor of the estate of a deceased individual, or a Federal, State, local or tribal law that establishes such authority (e.g., parent of a minor).

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

tt. **Personnel.** For the purpose of this directive, the term personnel includes officers and employees of VA; consulting and attending physicians; without compensation (WOC) workers; contractors; others employed on a fee basis; medical students and other trainees; and volunteer workers, excluding patient volunteers, rendering uncompensated services, at the direction of VA staff. ***NOTE:*** *Compensated Work Therapy (CWT) patients are part of VHA Vocational and Rehabilitation Services program. They are not VHA personnel; they are patients receiving active treatment or therapy.*

uu. **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.

vv. **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 protected health information 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.*

ww. **Psychotherapy Notes.** Psychotherapy notes are notes recorded by a 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 CFR 164.501). Psychotherapy notes may not be

used or disclosed without the prior written authorization of the individual to whom the notes pertain. Psychotherapy notes are not considered protected health information.

xx. **Record.** 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.*

yy. **Required by Law.** Required by law is 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.

zz. **Research.** Research is a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge.

aaa. **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.

bbb. **Sensitive Personal Information.** Sensitive personal information (SPI), with respect to an individual, means 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, social security number, 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."*

ccc. **Sickle Cell Anemia or Trait.** Sickle cell anemia or trait includes any activities relating to testing, diagnosis, treatment, or any other procedure relating to the disease of sickle cell anemia.

ddd. **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.

eee. **Subpoena.** 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.

fff. **Subpoena Duces Tecum.** 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.

ggg. **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.

hhh. **System Manager.** The System Manager is the VHA official 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, Procedures for Establishing and Managing Privacy Act Systems of Records. The VHA health care facility official with the program assignment is responsible for the maintenance of the records at the facility.

iii. **System of Records.** 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.

jjj. **Treatment.** 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.

kkk. **Unique Identifier.** A unique identifier is an individual's name, address, social security number, 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 individually-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:*** *The VA Office of General Counsel has indicated that the first initial of last name and last four of the social security number (e.g., A2222) is not a unique identifier; therefore, inclusion of this number by itself does not make the information identifiable or sensitive.*

lll. **VHA Health care Facility.** For the purpose of this directive, the term VHA health care facility encompasses all program offices and facilities, including but not limited to VISNs, VHA medical centers, VHA Health care Systems, Community Based Outpatient Clinics (CBOC), Readjustment Counseling Centers (Vet Centers), and Research Centers of Excellence under the jurisdiction of VHA.

mmm. **Without Compensation Appointment.** A WOC appointment is a personnel appointment under which an individual contributes time to VA activities but receives no monetary compensation.

nnn. **Work Study Students.** Work study students are individuals in paid capacity programs and are not patients. 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 required security training and complete a background check.

4. POLICY

It is VHA policy to conform to the legal requirements for using and disclosing individually-identifiable information and the appropriate handling of individuals' privacy rights regarding individually-identifiable information.

5. INDIVIDUALS' RIGHTS

a. **The Individual.**

(1) Individuals have the right to receive a VHA Notice of Privacy Practices concerning individually-identifiable health information. This notice must explain how VHA may use and disclose individually-identifiable health information, the individual's rights regarding the individual's individually-identifiable health information, and VHA's legal duties with respect to individually-identifiable health information.

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

(3) Individuals have the right to ask VHA to amend their individually-identifiable information including PHI when the PHI 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.(9).

(4) Individuals have the right to an accounting of disclosures of their individually-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 restrictions, but if it does, VHA must adhere to the restrictions 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 the Department of Health and Human Services (HHS), Office for Civil Rights (OCR), in accordance with 45 CFR 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 SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 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 Chief Business Office (CBO) Procedure Guide 1601B.02, Inpatient Care (Chapter 2, Section 2.E.4). http://vaww.va.gov/CBO/apps/policyguides/infomap.asp?address=VHA_PG_1601B.02.2.E.4 The Facility Directory Opt-Out does not apply to emergency rooms 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).

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 CFR Section 17.32(e) for authorized surrogates for informed consent). The following paragraphs provide details on various types of personal representatives for the purposes of this directive.

(1) **Power of Attorney.**

(a) 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 individually-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.

(b) Types of POA.

1. General Power of Attorney. A general power of attorney (GPOA) provides broad authority for the agent to act on behalf of the principal. A 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. The 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 POA. 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 power of attorney 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 powers of attorney enable a third-party to act on behalf of a Veteran claimant seeking benefits (including health care benefits) from VA (see 38 CFR 14.631).

3. Durable Power of Attorney for Health care (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: Living Will & Durable Power of Attorney for Health care, may be used to make such an appointment. Information about use of VA Form 10-0137 is found in VA Form 10-0137a, Your Rights Regarding Advance Directives, and VA Form 10-0137b, What You Should Know About Advance Directives. A durable power of attorney expires upon death of the individual.

(c) 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 powers of attorney must be:

a. In writing,

b. Signed by the 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, and

e. A specific designation, by name, of a third party agent, which may be an organization or entity, to act on behalf of the individual.

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. 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 Regional Counsel's office 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 Regional Counsel's office for guidance.

(2) **Legal Guardian.** Depending on the circumstances involved, a court may appoint a legal guardian for a specific purpose. 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 individually-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 un-emancipated minor), that person is considered a personal representative for the purposes of this directive. VHA may disclose individually-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. ***NOTE:*** *For disclosures of individually-identifiable information on a deceased individual see paragraph 34, Deceased Individuals.*

(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. ***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 receiving care at a VHA facility adequate notice of VHA's privacy practices. Information Bulletin (IB) 10-163, VHA Notice of Privacy Practices, is provided by the Health Eligibility Center (HEC), along with information on enrollment, to all Veterans enrolling in VHA for the first time. An individual has the right to request a copy of VHA Notice of Privacy Practice at any time. The 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 (e.g., humanitarian, non-VA research subjects, caregivers, and Servicemembers receiving care or treatment at a VHA 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. All non-Veteran patients must acknowledge receipt of the VHA Notice of Privacy Practices per VHA Handbook 1605.04, Notice of Privacy Practices.

c. Even if an individual has requested an electronic copy of VHA Notice of Privacy Practices, the individual still has the right to obtain a paper copy.

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. When an individual appears in person, the requirements are limited to 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. Currently, VHA policy does not allow an individual to verify identity by Email.

(2) In-person requests for information where suitable identification is not provided after it has been requested by VHA will be denied until appropriate identification has been provided.

(3) Requests for information via mail where suitable identification information, such as social security number 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 and/or Review of Records.**

(1) Requests for access to look at or review copies of individually-identifiable information must be processed in accordance with all Federal laws, including 38 U.S.C. 5701 and 7332, FOIA, Privacy Act, and HIPAA Privacy Rule. Except as otherwise provided by law or regulation, individuals, upon signed written request, may gain access to, or obtain copies of, their individually-identifiable information or any other information pertaining to them that is contained in any system of records or designated record set maintained by VHA. 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 must be received by mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed 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 of those positions.

(3) In determining whether to grant a right of access request, the appropriate 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 requested has been compiled in reasonable anticipation of a civil action or proceeding.

(d) 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).

(e) 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 by 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 security access log (Sensitive Patient Access Report or SPAR) contains employee names, a Veteran still has a first party right of access to the SPAR because the SPAR is covered under the Privacy Act system of records, "*Veterans Health Information Systems and Technology Architecture (*VistA)-VA" (79VA10P2).*

(5) Request for access to view a record must be processed as follows:

(a) When individuals appear in person at a VHA 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 a National Archives and Records Administration (NARA) Records Center 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, etc.), 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.

(c) Requests received by fax are acceptable only after confirmation has been obtained from the individual to whom the record pertains. 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 will determine whether access will be granted and the request will be processed in the same manner in which it was initially received at the facility, if emergent response is required, or as a request received via mail.

(d) When a request for records has been transferred or referred from another Federal agency or VA office to a VHA health care facility, the VHA health care facility will process the request in the same manner as a request received via mail.

(e) Email requests will not be accepted until such time as VHA can authenticate the identity of the Email sender and accept an electronic signature within an Email. The Electronic Signatures in Global and National Commerce Act, Public Law 106-229 addresses the requirements for a legally effective electronic signature. However, VA has not formally promulgated regulations that accepts an electronic signature on a Privacy Act records request (38 CFR 1.577(b) requires such requests to be "in writing"). VHA will issue formal policy guidance when electronic signatures are acceptable.

(f) A scanned 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 and Handbook 6500.

(g) Electronic requests received through VA information technology (IT) software and applications, such as My HealtheVet 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.

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

(a) A VHA employee must be present at all times 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 CFR 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 statement, using VA Form 5571, Authorization to Disclose a Record in the Presence of a Third Party, authorizing discussion of the record in the accompanying person's presence. If the record includes information that pertains to treatment for drug or alcohol abuse, HIV infection, or sickle cell anemia, an additional written authorization such as VAF 10-5345 Request for and Authorization to Release Medical Records or Health information is required.

(7) Time Frames.

(a) VHA health care facilities must process all requests for review or copies of individually-identifiable information within 20 working 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 working day time frame, an acknowledgment letter of the request to the requester must be sent within the same 20 working days.

(b) When, for good cause, a facility is unable to provide the requested information in a record within the 20 working day period, the individual must be informed in writing as to 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 working days from receipt of request.

(8) 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 CFR 1.577.

c. **Denial of Access.**

(1) A right of access request for a record may be denied in very limited circumstances.

(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) Provide the individual's appeal rights to the Office of General Counsel (024), 810 Vermont Ave., N.W., Washington, DC 20420, and

(c) Be signed by the VHA health care facility Director or official designee.

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 CFR 1.579 and 45 CFR

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.

(2) The written amendment request must be routed to the facility Privacy Officer or Chief, Health Information Manager (HIM). Amendment requests are to be maintained by the facility Privacy Officer per the Records Control Schedule (RCS 10-1) and must not be filed within the Veteran's health record unless, after denial of the amendment request, a Statement of Disagreement has been received from the Veteran or the Veteran has requested his amendment request letter and the facility's subsequent denial letter be affixed to the disputed record.

(3) 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.

(4) Name Change. A request for name change is considered an amendment request and must have the appropriate legal documents in order for the Master Veteran Index (MVI) Coordinator to make the change. The following documents, as outlined in VHA Directive 1906, are acceptable official supporting documentation for a name change; provided they are current (expired documents are not acceptable):

(a) A letter from the Social Security Administration (SSA) stating that all required documentation has been received and a new SSA card will be issued,

(b) A valid State Driver's license/State issued ID card,

(c) New SSA card with the name change,

(d) An official name change court order,

(e) An amended birth certificate, or

(f) A valid passport. ***NOTE:*** *Marriage licenses or certificates are not sufficient stand-alone documents for a name change as not all people who apply for a marriage license or marry change their official name.*

(5) The VHA staff member who authored the information that is the subject of the amendment request must review and determine whether to approve or reject the amendment request. In reviewing requests to amend, the author must be guided by the criteria set forth in 38 CFR 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 material to a record or to delete information from a record.

(6) When an individual requests amendment of clinical or health information in a health record maintained at a VHA health care facility, the Chief of HIM, or designee, or the facility Privacy Officer, or designee, must refer the request and related record to the health care provider who is the author of the information to determine if the record needs to be amended. If the health care provider is no longer on station, a health care provider designated by the VHA health care facility Director or Chief of Staff must determine if the record needs to be amended.

(7) Time Frames. A request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination whether to honor the request has not been made within this time period, the Chief of HIM, or designee, or 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 workdays 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 may not exceed 90 calendar days from receipt of the request.

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

(a) Any information to be deleted 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 CFR 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 amendment of a TIU (Text Integration Utility) document, the Chief of Health Information Management (HIM), or designee, is responsible for utilizing the TIU AMEND action for all TIU documents. Please refer to the TIU User Manual for specific instructions on utilizing the TIU amend functionality found on the HIM website. 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. Refer to Non-TIU Document Changes and Corrections Frequently Asked Questions (FAQ) for processes to correct Non-TIU documents.

(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 Chief of HIM, or designee, or the facility Privacy Officer, or designee, must notify the individual so that they can identify and agree to have VHA notify any relevant persons or organization that had previously received their information. If 38 U.S.C. 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations.

(d) In addition, the Chief of HIM, or designee, or 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.

(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.*

(9) Denial of Amendment Request. When a request to amend a record is denied, the Chief of HIM, or designee, or the facility Privacy Officer, or designee, must promptly notify the individual making the request of the decision. The written notification must:

(a) 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:

1. 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.

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

3. Is not part of a VHA system of records or designated record set.

(b) Advise the individual that the denial may be appealed to Office of the General Counsel (OGC) and include the procedures for such an appeal as noted below in paragraph 9.b.

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

(d) 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.

(e) Be signed by the VHA health care facility Director or official designee.

(10) If requested by the individual, the Chief of HIM, or designee, or 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.

(11) 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 the Office of General Counsel (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 should be reversed, in whole or in part, the individual and the VHA 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 HIM, or 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 individual must be advised, in the appeal decision letter, of the right to file a concise written statement of disagreement with the VHA health care facility that made the initial decision.

(4) A statement of disagreement can be done prior to appealing to OGC. A statement of disagreement must concisely state the basis for the individual's disagreement. ***NOTE:*** *Generally, a statement needs to be no more than two pages in*

length, except an individual may submit a longer statement if it is necessary to set forth the disagreement effectively.

(5) A VHA 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.

(6) 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 request for an amendment, the facility's denial of the request, the individual's statement of disagreement, if any, and facility's rebuttal, if prepared, must be appended or otherwise linked to the individual's record.

(7) 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, Chief of HIM, 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.

(8) 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 the VA's reasons for not making the amendments requested or rebuttal must also be provided.

c. **Documents for Facility Amendment File.**

(1) The facility Privacy Officer must keep all amendment requests for records maintained by their respective VHA health care facilities in an organized file by date. This file should contain 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 Statement of Disagreement,

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

(g) All provide 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) Facility written rebuttal to individual's Statement of Disagreement, if applicable,

(j) Any correspondence from the VA Office of General Counsel 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.* ***NOTE****: Amendment requests are not tracked in the ROI Plus software, because they are not considered disclosures.*

(2) The amendment files must be maintained for the life of the record. The amendment files are not scanned into the Veteran's health record as they are not considered part of the health record. They may be maintained in a secure and locked file cabinet or scanned to a secure network drive but cannot be scanned into the administrative portion of VistA Imaging in the health record.

(3) The amendment file must be retained and destroyed in accordance with RCS 10-1, Privacy Amendment Case File under Section XLIII-6.

9. ACCOUNTING OF DISCLOSURES FROM RECORDS

a. An individual may request a list of all disclosures of information, both written and oral, from records pertaining to the individual, subject to the provisions of 38 CFR 1.576(c) and 45 CFR 164.528. VHA health care facilities and programs are required to keep an accurate accounting for each disclosure of a record to any person or to another agency that is outside of VA including State reporting and research. For disclosures made for VHA research, the research investigator must be able to produce an accounting of disclosure upon request.

b. An accounting is <u>not</u> required to be maintained in certain circumstances, including when disclosure is to VHA employees who have a need for the information in the performance of their official job duties, under a traditional FOIA request, to the individual under Right of Access, or disclosure of a limited data set or de-identified data.

c. 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 VHA health care facility that maintains the record, and directed to the attention of the Chief of

HIM, or designee, or to the facility Privacy Officer, or designee, or the System Manager for the VHA system of records from which the accounting is being requested.

d. 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, and

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

e. 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 CFR 1.576(b)(7) and 45 CFR 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.*

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

g. VHA must retain a copy of the disclosure summary provided to the individual for six years or the life of the record (see Records Control Schedule (RCS 10-1) or the facility Records Control Officer).

h. The accounting or disclosure summary must be maintained via the automated ROI Plus software per VHA Directive 1615 , Mandated Utilization of Release of Information (ROI) Plus Software; on VA Form 5572, Accounting of Records/Information Disclosure Under Privacy Act, in a designated record set; or on an Excel spreadsheet located on a shared network drive.

10. CONFIDENTIAL COMMUNICATIONS

a. An individual has the right to request and receive communications (correspondence) confidentially from VHA by an alternative means or at an alternative location. 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.

b. VHA considers an alternative means to be in person (rather than by mail) and considers an alternative location to be an address other than the individual's permanent address listed in VistA.

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

d. If a Veteran requests to use his or her cell phone number as an alternate means of verbal communication, they should be directed to Eligibility Office within the VHA medical facility. Currently no electronic process to alert staff to use this number as an alternative "confidential" communication is available. ***NOTE:*** *A request to receive communications via Email is considered unreasonable and therefore will be denied. MyHealtheVet secure messaging should be used for this purpose.*

e. All communications or correspondence must 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, or

(5) All other.

f. Requests to have all communications or just communications of a specific correspondence type, sent to the "confidential communications" address must be accommodated. 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.

11. RIGHT TO REQUEST RESTRICTION

a. An individual has the right to request VHA to restrict its use or disclosure of individually-identifiable health information to carry out treatment, payment, or health care operations. An individual also has the right to request VHA to 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. Health care providers are prohibited from granting any verbal restriction requests. Documenting in the Veteran's health record does not constitute a restriction request.

b. Generally, VHA would not agree to grant an access restriction by a personal representative of a deceased Veteran to restrict a family member's access under FOIA.

c. VHA is not required to agree to any restrictions. ***NOTE:*** *45 CFR 164.522(a)(1)(vi) does not apply to VHA.*

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.

e. Before granting any request for restriction of individually-identifiable health information, the VHA facility Privacy Officer must review the request and consult with the VHA Privacy Office by telephone or Email. 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 11j. 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 the Computerized Patient Record System (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, because other legal authorities, such as emergency care may require the disclosure.

j. VHA may terminate a 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 protected health information 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. **VHA.**

(1) For purposes of this directive, individually-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 requires a written authorization or other authority as described in this directive.

b. **VA Entities.**

(1) **Individually-Identifiable Information Excluding Health Information.** VHA may share individually-identifiable information, excluding health information, to any component of VA that needs the information for the purposes of fulfilling the agency's mission without signed, written authorization.

(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 treatment, payment, or health care operations without the signed, written authorization of the individual as long as a national Business Associate Agreement (BAA) is in effect. For example:

1. VHA Central Office must maintain a national BAA with OGC for authorizing the disclosing of individually-identifiable health information with OGC for legal counsel provided to VHA.

2. VHA Central Office must maintain a national BAA with the VA Office of Information and Technology (OI&T) for authorizing the disclosing of individually-identifiable health information with OI&T for IT services, security services, and incident response. ***NOTE:*** *Before disclosing protected health information, contact the VHA Health Information Access Office to confirm the existence of a business associate agreement or check online at*: *http://vaww.vhadataportal.med.va.gov/DataAccess/BusinessAssociateAgreements.aspx This is an internal VA Web site that is not accessible to the public.*

c. **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 business associate agreement 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 individually-identifiable information to a VA contractor to ensure appropriate authority is in place.

(4) For guidance on business associate agreements, see VHA Handbook 1605.05, Business Associate Agreements.

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

d. **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 authorization is obtained.

13. RESEARCH

This paragraph is meant to provide guidance only with regards to the Federal privacy and confidentiality laws affecting research endeavors. Each VHA health care facility must establish a review process to ensure these privacy requirements are met. The review process may involve the facility's Privacy Officer being a non-voting member of the facility Institutional Review Board (IRB) or Research and Development (R&D) Committee or a member of another research subcommittee responsible for ensuring that all privacy and security requirements are met. The facility Privacy Officer is responsible for reviewing the 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. The facility Privacy Officer is not responsible for the approval of the informed consent for research purposes. This policy 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:*** *See VHA 1200-series Handbooks and directives 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. 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 facility's Associate Chief of Staff (ACOS) for R&D.*

(2) Reviews Preparatory to Research. VA Investigators may use individually-identifiable information to prepare a research protocol prior to submission of the protocol to the IRB 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 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.

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

4. A DUA may be required if individually-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 subparagraph and returns or destroys the individually-identifiable information once the review is completed. See VHA Handbook 1200.12, Use of Data and Data Repositories in VHA Research.

5. 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.

(3) VA-Approved Research. All non-exempt research activities involving human subjects conducted by VA Investigators must be approved by an IRB and R&D Committee prior to initiation of the research in accordance with VHA Handbooks 1200.01, Research and Development (R&D) Committee, and 1200.05, Requirements for the Protection of Human Subjects in Research, and 38 CFR part 16. 38 CFR part 16 is VA's implementation of the federal regulation for the protection of human subjects commonly referred to as the "Common Rule". In addition to the review requirements in

part 16, the Information Security Officer and facility Privacy Officer must also review the research to ensure it is in compliance with all applicable security and privacy requirements related to the security safeguards and confidentiality of the information to be used and disclosed.

(4) All VA Investigators conducting VA-approved research must obtain appropriate legal authority to use individually-identifiable information, including health information, and to disclose individually-identifiable information outside of VA as part of the VA-approved research.

(5) VHA individually-identifiable health information involving non-employee research subjects (e.g., Veterans, their beneficiaries, and patients) may be used by a VA investigator for research purposes provided there is a prior written authorization that meets all requirements as identified in paragraph 14 of this directive. A written authorization may not be incorporated into an informed consent for participation in research, because the signature authorities are not the same for each document. ***NOTE:*** *See VHA Handbook 1200.05 for guidance on who can sign an informed consent for participation in research.*

(6) If there is no prior signed, written 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 CFR 164.512(i). A waiver requires that the IRB or Privacy Board appropriately document that it has determined that the waiver of 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 the PHI.

(d) A summary of the PHI to be used or disclosed. ***NOTE:*** *The IRB's documentation must be signed by the IRB Chair or other designated voting member of*

the IRB. VHA Form 10-0521, IRB Documentation of Waiver of HIPAA Authorization for Research, should be used for this documentation.

(7) VHA individually-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, Veterans Health Administration Research and Development Program, applicable 1200 series Handbooks, and 38 CFR part 16.

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

(9) 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.

(10) VA Investigators may use and disclose the requested data only in a manner consistent with the approved research protocol or informed consent form for which the information was requested.

(11) VA Investigators may use individually-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 separate HIPAA authorization must be obtained once the subject is recruited but before any other research interventions take place.* VHA Handbook 1200.05 states other requirements that must be met for recruitment of research subjects.

(12) If a research subject properly executes a written authorization for disclosure of his or her protected health information 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 Data Use Agreement); ownership of the disclosed data transfers to the recipient and VA cedes control over the information.

(13) A waiver from the VA Chief Information Officer must be obtained before VA sensitive 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 student as part of studies in a classroom setting, thesis, etc. Case reports or case studies should contain only de-identified information or pictures that totally conceal the identity of the individual. If personally identifiable information (PII) 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 should consult with the facility Privacy Officer to ensure that all information is appropriately de-identified as required by the HIPAA Privacy Rule. The 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 should be consulted*. See VHA Handbook 1200.05 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 Data Use Agreement 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.

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 VHA health record, then these copies are covered under the Privacy Act SORN 24VA10P2, 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. **ROI for Non-VA Investigators (Extramural).** VHA has authority to disclose individually-identifiable information to non-VA investigators in accordance with this directive and the applicable Privacy Act System of Records. The request must be for a specific research study.

(1) **Reviews Preparatory to Research.** A non-VA 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, and patients) to non-VA Investigators for research purposes provided there is a prior signed, written authorization.

(b) Disclosure to Federal Investigators (Researchers). If there is no prior signed, written authorization, VHA may disclose individually-identifiable health information to

non-VA Federal investigators (researchers) (e.g., Department of Defense, 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 CFR 164.512(i) prior to the request for the individually-identifiable health information.

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

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 CFR 1.488 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 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.

2. The research has been approved by the investigator's IRB of record and an IRB or Privacy Board has waived the requirement for a HIPAA authorization in accordance with 45 CFR 164.512(i) prior to the request for the individually-identifiable health information.

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

4. When 38 U.S.C. 7332-protected information is also requested, the non-VA, non-Federal investigators must submit written assurance in writing that the purpose for requesting data is to conduct scientific research and the requirements in 38 CFR 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.

(d) Requirements of 38 CFR 1.488. Title 38 U.S.C. 7332-protected information may be disclosed without written authorization if, in addition to the above applicable

requirements, the requirements of 38 CFR 1.488 are met. Specifically, the written assurance must indicate:

1. The information must be maintained in accordance with the security requirements of 38 CFR 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) VHA may disclose a limited data set for research pursuant to a DUA, if the research has been approved by the investigator's IRB of record.

(f) Requests for de-identified information from non-VA Investigators must be in writing and meet the requirements of Appendix A. These requests are FOIA requests and should be processed in accordance with FOIA.

(g) If the research does not meet the definition of Human Subject Research per the Common Rule (38 CFR 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 individually-identifiable information of research subjects in their capacity as VHA employees, excluding health information, to non-VA Investigators for research purposes without written authorization, and only in accordance with the Privacy Act 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 using the same privacy processes as Veteran health information.

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

(c) VHA 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:*** *Adults filing online for Social Security disability benefits on their own behalf are able to 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.*

(2) The written authorization must comply with all the requirements of paragraphs 14.b. through 14.h.

(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 individually-identifiable information, the authorization must be in writing and include the following information:

(a) The identity, e.g., name and social security number, of the individual to whom the information pertains. If the full name (first, middle, last) is on the authorization, the entire social security number is not required. The last four of the SSN will be required for purposes of filing the document into the Veteran's health record.

(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 is to be disclosed, this information must be specifically identified in the description.

(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.

(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.

(e) A description of each purpose of the requested use or disclosure. A statement "at the request of the individual" is sufficient when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(f) An expiration date or event that relates to the individual or the purpose of the use or disclosure. VA Form 10-5345, Request for and Authorization to Release Medical Records, supplies three possible expiration options: 1) upon satisfaction of the need for the disclosure; 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 individually-identifiable health information for research.

2. The statement "none" or similar language is sufficient if the authorization is for the agency to use or disclose individually-identifiable health 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. For purposes of billing where an authorization is needed for 38 U.S.C. 7332-protected conditions, an expiration date of 5 years is acceptable.

4. For purposes of enrolling Veterans in the Veterans Lifetime Electronic Record (VLER) Health Exchange and VA Form 10-0485, Request for and Authorization to Release Protected Health Information to eHealth Exchange is needed for 38 U.S.C. 7332-protected conditions, an expiration date of 10 years is acceptable. ***NOTE:*** *Each VHA facility must have a process in place to monitor authorization expiration dates.*

(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 of disability, the authorization 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 authenticate the authorization. If no symbol or mark can be made by the individual, the authorization form must briefly document the circumstances of the signature and two adult witnesses to authenticate the individual's intent to provide authorization.

(h) The date signed by the individual or his personal representative. The authorization should 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 CFR 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 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.

(2) Authorization may be given on VA Form 10-5345, Request for and Authorization to Release Medical Records or Health Information, or any HIPAA Privacy Rule-compliant authorization form or any correspondence, provided it meets all the requirements noted above in paragraph 14b. to be considered a valid authorization.

(3) If the authorization is for research purposes, VA Form 10-0493 Authorization for Use & Release of Individually Identifiable Health Information for Veterans Health Administration (VHA) Research should be used. ***NOTE:*** *Photocopies, scanned documents, or faxes of authorizations forms are acceptable after the validity of the form has been verified by the Release of Information 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 on the basis of 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 or 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 needs to be known, to VHA personnel to be false or inaccurate with respect to any item of the authorization requirements, or

(h) Is not signed. 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 release of information 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 individually-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, individually-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, but the authorization must explicitly include language to this effect.

(3) If an individual dies prior to executing the authorization, the authorization is not valid.

f. **Authorization Content Requirements for HIV, Sickle Cell Anemia, Drug and/or 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 34).

(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 a person is undergoing treatment for a unrelated medical condition, such as a knee replacement, but informs the health care provider of a history of 38 U.S.C. 7332-protected information and their current treatment plan does not address treatment or referral of any one of these section 7332-protected conditions, then the current treatment documentation may be disclosed without a special authorization.

(4) If a patient with alcoholic delirium tremens is admitted for detoxification treatment and is subsequently released with no counseling or referral to a substance abuse treatment program, no special authorization is required.

(5) If the patient is being treated for pain management and a provider performs a drug toxicology screen with no counseling, treatment or referral for an underlying condition of drug abuse, no special authorization is required.

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 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) VHA is not required to review all of the individually-identifiable information being disclosed pursuant to a signed, written special authorization in order to ascertain whether 38 U.S.C. 7332-protected information is included in the disclosure.

(3) The notification must inform the person that anyone who violates any provision of 38 U.S.C. 7332 will be fined up to $5,000 in the case of a first offense, and up to $20,000 in the case of a subsequent offense.

(4) The person to whom name and address information is disclosed must be notified in writing that the information may not be re-disclosed or used for a purpose other than that for which the disclosure was made under 38 U.S.C. 5701(f).

h. **Compound Authorizations.**

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

(a) Except as set forth in paragraph 14.h.(2) below, 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 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) An authorization for the use or disclosure of individually-identifiable health information for a research study may not be combined with the Research Informed Consent.

(3) 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 and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditioned authorization. ***NOTE:*** *VA investigators are not required to combine authorizations for the research study. Separate authorizations may be used.*

15. PROCESSING A REQUEST

a. **General.**

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

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

(3) If the requester is the individual to whom the records pertain, follow the guidance regarding individual's right of access under paragraph 7.

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

(a) If the record requested does not contain individually-identifiable information, refer the request to the facility FOIA Officer for processing of the request under the FOIA.

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

(c) If the record requested contains individually-identifiable information and the guidance in paragraphs 16 through 34 is not applicable to the request, process the request by reviewing the applicable Federal privacy laws and regulations as indicated in paragraph 17, ROI Outside VA, for any Purpose. If there is not explicit disclosure authority other than under the FOIA, then process the request as a FOIA request.

(d) If the request is for records related to a deceased individual, process the request in accordance with paragraph 34, Deceased Individuals.

(5) Process requests from a third party for individually-identifiable information within the required time standards outlined in paragraph 15.b. and charge the applicable fees outlined in paragraph 15.c. if an appropriate authority has been identified to allow the disclosure.

(6) A third party may request VHA to disclose or provide individually-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 particular request for individually-identifiable information is not clearly identified within this directive, contact the facility Privacy Officer for assistance.*

b. **Time Standards.**

(1) Requests for copies of individually-identifiable information, including health information, must be answered within 20 workdays from the date of receipt. Date of receipt is the date the request was actually received by the VHA health care facility department or employee able to process the request. The request must be date stamped or a manual date must be placed upon the request.

(2) When, for good cause shown, the information cannot be provided within 20 workdays from the date the request was actually 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 workdays.

(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, Individual's Right of Access.

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 requesters in connection with processing FOIA requests are addressed in the FOIA Handbook. 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 CFR 1.577(e) or subsequent regulations will be charged.

(2) **Table of Fees.** (This table only applies if fees exceed $25.00 per 38 CFR 1.561).

ITEM	COST
Privacy Act: for health records by patient, guardian or personal representative	• First copy free then $0.15 per page after the first 100 one-sided pages for subsequent copies of the same records • Free in support of a VBA claim on appeal • No search or review fees
Privacy Act: for a PA System of Records other than health record filed and retrieved under the requester's identity **or** a third party requester, i.e. attorney, for any PA System of Records, not seeking the records in support of a VBA claim on appeal	• First 100 one-sided pages free then $0.15 per page • No search or review fees
Non-*paper* copies (x-rays, video tapes, slides, microfilms, disk computer files, etc.)	• Actual direct cost of duplication
Attestation under the seal of the Agency, i.e. VA notary	• $3.00 per document
Abstracts or copies to insurance companies for other than litigation purposes	• $10.00 per request

NOTE: *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 percent 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 Regional Counsel.** The following types of requests for information must be reviewed with the Regional Counsel and any release of information will be made only in compliance with the instructions of Regional 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 Regional 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 CFR 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) should 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 information, see VHA Chief Business Office (CBO) Procedure Guide 1601C.03.8.H.3.c-f, Revenue for Veteran Benefits/Claims, Workers' Compensation/Tort Feasor/No-Fault Reasonable Charges and Billing Guidelines.

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

This paragraph covers the use and disclosure of individually-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 operation. 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.

a. **Veterans Benefits Administration.**

(1) VHA may disclose Veteran's individually-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 CFR 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.

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

c. **National Cemetery Administration.** VHA may disclose individually-identifiable information to the National Cemetery Administration (NCA) for eligibility for, or entitlement to, or that provide benefits under the laws administered by the Secretary of Veterans Affairs (see 45 CFR 164.512(k)(1)(iii). For example, VHA may provide NCA claimant information for burial benefits.

d. **Office of General Counsel.**

(1) VHA may provide all information, including individually-identifiable information and 38 U.S.C. 7332 information, to the Office of General Counsel (OGC) for any official purpose authorized by law.

(2) VHA must maintain a national BAA with OGC for authorizing the sharing of protected health information with OGC for legal counsel provided to VHA.

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 individually-identifiable information to OEDCA when necessary for determining compliance with Equal Employment Opportunity (EEO) requirements.

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

(1) VA Office of Inspector General (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 individually-identifiable information, to the VA Inspector General for any official purpose authorized by law. The individually-identifiable health information includes 38 U.S.C. 7332-protected health information for the purpose of health care oversight (see 45 CFR 164.512(d)). Unless otherwise specified by the VA OIG, all requests for VHA individually-identifiable health information should be for health care oversight activities. The VA OIG is not required to provide VHA with a written request for health care oversight activities.

(3) For guidance on disclosures to the VA Inspector General for purposes of law enforcement activities, see paragraph 21.i. on VA Police and VA OIG (see 45 CFR 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 protected health information.

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

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

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

h. **VHA Office of Medical Inspector.** The VHA Office of Medical Inspector (OMI) addresses health care problems to monitor and improve the quality of care provided by VHA. VHA must provide any information, including individually-identifiable information and 38 U.S.C. 7332-protected health information to VHA OMI for their reviews which are generally related to treatment, health care operations and health care oversight. The OMI is not required to provide a written request.

i. **VHA Office of Research Oversight.** 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 provide a written request for protected health information or other individually-identifiable information when needed in connection with its compliance oversight responsibilities.

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

(1) The U.S. Office of Special Counsel (OSC) is an independent agency that enforces Whistleblower protections, safeguards the merit system and provides a secure channel for whistle blower disclosures.

(2) OSC may accept Whistleblower disclosures and require VHA to investigate these disclosures.

(3) VHA may disclose individually-identifiable information to investigators who have been tasked to investigate the Whistleblower complaint.

(4) VHA may disclose individually-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 (b)(7) letter.

k. **VA Contractors.**

(1) VHA may disclose non-Veteran individually-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 individually-identifiable information apply to the VA contractor.

(2) The facility Privacy Officer must be contacted prior to the release of any Veteran individually-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. The facility Privacy Officer will collaborate with the Information Security Officer and Contracting Office Representative (COR) on all contracts, new or revised.

(4) All contracts that provide for the maintenance of 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 (VAAR). VHA 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) Contract Nursing Homes. A nursing home with which VHA has a contract may be provided individually-identifiable information including health information for the purpose of fulfilling the contract for providing health care to Veterans housed in its facilities.

l. **VA Human Resources Management Services.**

(1) VHA may disclose individually-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)Occupational Health 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 purposes of managing the VHA work force under a business associate relationship.

m. **VA Police Service.**

(1) VHA may provide VA Police Service with individually-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 VHA medical facility appointments, searching for missing Veterans, or subduing Veterans. No special request or other documentation is needed.

(2) VHA may disclose individually-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) seeking care from the VHA medical facility. For these law enforcement functions, the facility VA Police Service must follow polices outlined in paragraph 21, Law Enforcement Entities.

(3) VHA may provide VA Police Service with individually-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 the VA Police Service is reasonably able to prevent or lessen the threat.

(4) Disclosure of individually-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) VA Police Chief, or designee, should only be given minimum access to VistA, such as to the Patient Inquiry Option. Access to CPRS is not appropriate. If protected health information about an individual is needed, the VA Police should contact the facility Privacy Officer.

n. **VA Researchers.**

(1) VHA may use employee information, including health information for official VHA research studies, in accordance with VHA Directive 1200, Veterans Health Administration Research and Development Program and 38 CFR part 16.

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

o. **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 VHA health care facility. This might include releasable portions of completed Administrative Boards of Investigation (AIB), 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) Types of Requests. 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 the Freedom of Information Act or without citing any particular statutory or contractual provision.

(3) Processing of Request. 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 Regional Counsel's office needs to be contacted immediately. The Regional 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 Regional Counsel staff can refer to the FOIA Handbook for guidance in how to process union requests for information or agency records.

17. ROI OUTSIDE VA, FOR ANY PURPOSE

a. **Disclosure with Authorization.**

(1) If VHA receives a request for individually-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.

(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 or VLER Authorization, but is not mandatory.

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

(1) This directive covers the disclosure of individually-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 individually-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 five 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 testing 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?

(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 the FOIA also applies to the request, disclosure is mandatory unless a FOIA exemption applies. See VA Handbook 6300.3, Procedures for Implementing the Freedom of Information Act, 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 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.

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 Congressman's assistance.

(a) When a constituent service request is received, VHA may disclose individually-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 should also include a copy of the constituent's inquiry to the Congressman 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 "Patient Medical Records-VA" 24VA10P2, Routine Use 9 and 45 CFR 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 14b.

(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) Constituents' 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, Social Security Number (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 Power of Attorney, 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 18a.(2). The

correspondence must have been submitted by the individual to whom the information pertains or by his or her 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 Congressman 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 individually-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 Oversight 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 individually-identifiable information is provided, the VHA official providing the information should 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 CFR 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 CFR 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 CFR 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 CFR 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.

(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 CFR 1.511 and 38 CFR 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 Regional 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 law suit, must be referred to Regional Counsel. This is a regulatory requirement and cannot be waived per 38 CFR 1.511(c). Contact the appropriate Regional 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 VHA 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 is not sufficient authority 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, upon advice from the Regional Counsel, either personnel from the VHA health care facility or the Regional Counsel 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) If 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., or VA does not retrieve the record by the name of the record subject or another identifier assigned to that individual), VHA may disclose records, excluding 38 U.S.C. 7332-protected information. Regional Counsel should 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 is made in response to a subpoena without the signed, written authorization of the individual, the VHA 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 you determine 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 VHA health care facility receives an order or a subpoena, the VA health care facility should immediately contact Regional Counsel for guidance.*

c. **Quasi-Judicial Bodies.**

(1) VA may disclose any individually-identifiable information to a quasi-judicial body in accordance with Federal policy and the 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, i.e. Social Security Administration, Federal Merit Systems Protection Board, and state Workers' Compensation Boards.

(2) An order from a Federal or State quasi-judicial agency is not a court order. 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 Court or in Quasi-Judicial Proceedings.**

(1) Original VHA records must remain in the custody of a VA employee at all times. An employee who merely 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. It is advisable to prepare a photocopy of the information or record. If the judge or the attorney requests the entire original record or part of the 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 records or any portion thereof, immediately contact Regional Counsel 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 CFR 1.522 whether disclosure of any part of the record 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) VHA health care facilities must develop procedures related to employees presenting testimony or VHA records in court. The assistance of the Regional Counsel must be requested in developing these procedures to ensure compliance with VA regulations and State requirements.

f. **Individually-Identifiable Information Protected by 38 U.S.C. 7332.**

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

(a) Individually-identifiable information or records that relate to treatment for drug abuse, alcoholism or alcohol abuse, or sickle cell anemia, or testing and 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 CFR 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 VHA 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 VHA health care facility, after consultation with Regional Counsel, may provide the court expert evidence from VHA health care professionals 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 CFR 1.493(e)).

(2) **Information Obtained for Research, Audit, and/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 individual information 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 20f.(4)(c) is sought with an order under this paragraph 20d, 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 VHA 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 Regional 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 VHA health care 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.

(c) 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 should be addressed with the employees' local payroll office once determination is given by the local Regional Counsel that the employee is required to attend.

j. **Competency Hearings.**

(1) VHA may disclose individually-identifiable health information to private attorneys representing Veterans rated incompetent or declared incapacitated for a competency hearing when a subpoena, discovery request or other lawful process is provided, as long as the individual has been given notice of the request. There is no authority to disclose to family members or a family member's attorney for the sole purpose of obtaining guardianship.

NOTE: *A subpoena does not meet the Privacy Act requirement. The Privacy Act authority for this disclosure is Routine Use number 8 under the "Patient Medical Records-VA," 24VA10P2 system of records. The subpoena is the authority under the HIPAA Privacy Rule since Privacy Act routine uses, by themselves, are not adequate authority for disclosure under the HIPAA Privacy Rule.*

(2) VHA may disclose individually-identifiable health 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 CFR 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 Veteran a notice.

(4) The Veteran whose competency is in question cannot authorize disclosure of his or her 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 patient's next-of-kin for a competency hearing unless the next-of-kin is a personal representative of the patient.*

k. **Litigation Holds.**

When a litigation hold is received from the Office of General Counsel, VHA health care facilities are required to maintain and preserve the information and data potentially relevant to the investigation until litigation has been resolved. Facility Privacy Officers should work with their Records Manager to ascertain what local facility information is available and any information that may be maintained by a local Business Associate. The Health Information Access Office will be responsible for notifying all National Business Associates. Check with Regional 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, individually-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, taking into account:

(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 may 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, 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.

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

(3) A qualified representative of the agency must make a written request which states 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 for which records are sought, and signed by a qualified representative of the agency. All requirements in this section of the Handbook must be met for the Standing Written Request Letter to be valid.

(4) 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. 570l(f). If the requester does not indicate awareness of this penalty provision in the request, disclosure of medical 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 VHA 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) Health care facilities will 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 in the letter. The request letter must be updated in writing every 3 years.

(6) If the facility receives an unsolicited standing written request letter and it does not meet the requirements of the template letter then the VHA health care facility Director, or designee, must acknowledge the receipt of an agency's standing request letter and advise the agency of the penalties using the language in the preceding paragraph regarding the misuse of the information and that the request letter must be updated in writing every 3 years.

(7) A file must be maintained for all standing written request letters submitted for information under the provisions of this paragraph. The facility Privacy Officer should work with the VA Police Chief to ensure that standing written request letters are created and maintained as appropriate, with both parties keeping a copy of the current letter on file.

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

(9) An accounting of disclosures must be maintained for all disclosures made pursuant to a standing written request letter (see paragraph 9).

(10) The standing written request letter authority under 38 U.S.C. 5701(f) and the corresponding published routine use in VA's Privacy Act systems of records are only for standing written request letters for routine reporting purposes. Standing written request letters and Privacy Act (b)(7) letters are not the same. See the guidance in paragraph 21.c. for Privacy Act (b)(7) letter requirements.

c. **Specific Criminal Activity, 5 U.S.C. 552a(b)(7).**

(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 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, 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. The delegation may only be to an official of sufficient rank to ensure that the request for the records has been the subject of a high-level evaluation of the investigatory need for the information versus the invasion of personal privacy involved. The requester must supply a copy of the written delegation of authority or provide a reference to the delegation such as a CFR Regulation 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 Regional 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) should 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, etc.

(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 tin the request. If the requester does not indicate awareness of this penalty provision in the request, disclosure of medical information under paragraph 28.b.(1)(b) 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 VHA 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 Regional Counsel may be sought, when appropriate, in evaluating the applicable law relative to the statutory authority of a governmental 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 in

response to a written request that meets the requirements of preceding paragraph for Specific Criminal Activity.

(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) Social security number;

(d) A, B, and O blood type and RH factor;

(e) Type of injury;

(f) Date and time of treatment;

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

(h) Description of physical characteristics.

NOTE: *This information may be provided to VA Police Officers and VA OIG Officials* without a written request.

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 it is own initiative individually-identifiable information to local law enforcement in order to locate missing patients. This information would include name, height, weight, hair color, clothing when last seen, and a Veteran Health Identification Card 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, or subsequent policy issue, establishes the policy to ensure that each VHA 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 Veterans Health Identification Card (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 VHA health care 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 prior 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 21c., VHA needs to 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 medical personnel have no authority to conduct chemical testing on patients for law enforcement purposes. However, VA personnel 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 personnel should 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, Regional Counsel needs to 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.

(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 individually-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 individually-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 CFR 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 use of 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.*

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 VHA health care facility, patient, or employee.

(2) Announcement at Arrival. All non-VA law enforcement officials entering the VHA health care facility should be directed to the Office of the Director, Chief of Police, or the Chief of Human Resources Management Service 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 OIG and VA Police).** VHA may disclose individually-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 individually-identifiable information pursuant to a standing written request letter (e.g., fugitive felon reporting (see VHA HB 1000.02, VHA Fugitive Felon Program).

(2) Specific Criminal Activity. VHA may disclose individually-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, social security number, 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 individually-identifiable information to VA Police when VHA believes the information constitutes evidence of criminal conduct that occurred on VHA grounds.

(5) Serious 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.

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 controlled premises and to conduct administrative inspections.

(2) Such entries and inspections shall 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.

(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 COLLECTION FUND

a. **Third-Party Claims (Tort Feasor, 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, excluding 38 U.S.C. 7332-protected information, from the health record to the extent required to effect recovery of the costs for medical care provided to patients in cases in which a third party, such as a tort feasor, 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, excluding 38 U.S.C. 7332-protected 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) Title 38 U.S.C. 7332 applies to all diagnoses, or other information that identifies, or could reasonably be expected to identify, a patient as having a drug or alcohol abuse condition, infection with HIV, or sickle cell anemia, but only if such diagnosis or information is received, obtained or maintained for the purpose of seeking or providing treatment for alcohol abuse, or such treatment has been offered and it was declined. Testing for HIV or sickle cell anemia trait is protected under this statute including tests with negative results.

(3) For 38 U.S.C. 7332-protected information (drug or alcohol abuse, HIV, or sickle cell anemia health information), the individual's signed, written authorization must be obtained prior to submitting the information to the third party or Federal agency and government-wide third-party insurer for payment purposes. VHA staff may not redact or delete information from the individual's record unless delegated this authority by your local FOIA Officer.

(4) Health care Effectiveness Data and Information Set (HEDIS). 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 will 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.

(5) The Civilian Health and Medical Program (CHAMPVA) is administered by the Chief Business Office (CBO), which is a part of VHA. Therefore, VHA is not required to obtain an authorization for disclosure under 38 U.S.C. 7332-protected information if CHAMPVA is the primary third party payer. If the CHAMPVA beneficiary has other health insurance as the primary payer and CHAMPVA as the secondary payer, then a special authorization would be required prior to disclosing 38 U.S.C. 7332-protected information to the other health insurer.

(6) VA Form 10-5345. Request For and Authorization to Release Medical Records, can be used as the authorization for the disclosures of 38 U. S. C. 7332-protected information for past, present, and future appointments when there is a condition or event and an expiration date. The expiration date should be no more than 5 years into the future.

(a) If the patient does not have a 38 U.S.C. 7332-protected condition in his record, then an authorization permitting the future disclosure of this information in the event the patient may contract one of these conditions is prohibited. An individual cannot check the boxes on the VA Form 10-5345 prior to the existence of the 38 U.S.C. 7332-protected condition when it does not currently exist.

(b) VA personnel must not require patients to complete a VA Form 10-5345 as part of the routine inpatient admission process. Patients with 38 U.S.C 7332–protected information may be offered the opportunity to voluntarily complete the form at the time of admission for administrative purposes (e.g. billing, utilization review).

(c) The Veteran must fill out VA Form 10-5345 in order for it to be valid. VHA staff cannot check the 38 U.S.C 7332-protected diagnosis boxes unless the person is standing in front of them or is on the phone with them, and the individual is directing VHA staff on the individual's behalf.

(7) In cases where a substantial bill is involved (i.e., $25,000 or more) consideration may be given to seeking a court order (see 38 U.S.C. 7332(b)(2)(D)) to permit disclosure. Such cases must be discussed with the Regional Counsel.

(8) For the purpose of VA collecting the cost of medical care, individually-identifiable health information, excluding 38 U.S.C. 7332-protected information, may be disclosed to a Federal agency or non-VA health care institution or provider that referred the patient when the medical care is rendered by VA under the provisions of a contract, sharing agreement, or individual authorization. Such disclosures may be made without written authorization. The patient's written authorization must be obtained to disclose 38 U.S.C. 7332-protected information.

(9) Accounting of Disclosure. An accounting of all disclosures of information contained in bills generated from the Integrated Billing Package is maintained as part of the billing system. Any other disclosure of health information requires an accounting of disclosure within the ROI Plus software or a separate tracking spreadsheet. Consult the facility Privacy Officer for additional information.

c. **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 Business Associate Agreement.

(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 the 10-10EZ, Application for Health Benefits, prior to the incurring a cost for care.

23. NEXT-OF-KIN, FAMILY AND OTHERS WITH A SIGNIFICANT RELATIONSHIP

a. **General Inquiry.**

(1) Appropriate VHA health care providers 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 or 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 individually-identifiable information including health information to next-of-kin, 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.

(2) VHA employees are encouraged to document the decision to share information 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, family members, and others with a significant relationship to the individual to whom the information pertains, without authorization, when, in the exercise of health care providers 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.

(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, 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 when good medical and ethical practices dictate.

d. **HIV Status Notification.**

(1) The 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 CFR 164.512(j) and 38 U.S.C. 7332(f)).

(2) Disclosure under this paragraph may be made only if the 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 health care provider, if the 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 treating health care provider or professional counselor must document, in the progress notes of the health record, the factors that are considered which lead 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) HIV Status Notification to a VA Employee. VA employee 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 may not record the source in the employee’s medical file unless authorization is obtained from that source.

(7) Disclosures to non-VA employees will 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 Information.**

(1) A VA health care provider 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 CFR 164.512(j), 38 U.S.C. 7332(b)(2)(F) and 38 CFR 1.484).

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

24. NON-VA HEALTH CARE PROVIDER (HEALTH CARE PROVIDERS, HOSPITALS, NURSING HOMES)

a. VHA may disclose individually-identifiable health information, excluding 38 U.S.C. 7332-protected 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 individually-identifiable health information, excluding 38 U.S.C. 7332- protected information, to a non-VA health care provider without the prior signed, written authorization of the individual to whom the information pertains for treatment of such individual, including a Veteran, Veteran beneficiary, member of the armed forces, or any other person who has received care from VA. When a non-VA health care provider needs a copy of individually-identifiable health information, the non-VA health care provider should submit a signed, written request as required by 38 U.S.C. 5702 and for tracked in the ROI Plus Software.

c. VHA may disclose individually-identifiable health information, excluding 38 U.S.C. 7332-protected information, to resident care homes, nursing homes, assisted living facilities, and home health services for the purposes of health care referrals without the signed, written authorization of the individual to whom the information pertains.

d. VHA may disclose 38 U.S.C. 7332-protected information to a non-VA health care provider including home health services, resident care homes, and assisted living facilities only with the signed, written authorization of the individual to whom the information pertains.

e. VHA may disclose protected health information including 38 U.S.C. 7332-protected information to a non-VA health care provider who referred his or her patient to VHA for treatment and subsequently seeks follow-up information regarding the Veteran's treatment.

f. VHA may disclose 38 U.S.C 7332-protected health information to a non-VA health care provider caring for an individual under emergent conditions.

g. 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.

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 the 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 VHA health care facility.

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

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

(4) The VHA 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 the OPO do not meet the intent for determining suitability based on the above four requirements above. If the 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 information, which will be withheld under Exemption 3 of the FOIA.

c. An accounting of disclosure is required when disclosing information to the OPO. An OPO is considered a health care provider, not a business associate of VHA.

d. For additional guidance contact the facility OPO coordinator (see 38 CFR 1.485a).

26. OTHER 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 Servicemember to the American Red Cross, for the purpose of justifying emergency leave of the active duty Servicemember. Information protected by 38 U.S.C. 7332 may not be disclosed for this purpose.

b. **Bureau of Census.** VHA may disclose individually-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 HIPAA Privacy Rule 164.512(a) and 5 U.S.C. 552a(b)(4)).

c. **Department of Defense (DoD).**(1) Military Command Authority. The Military Command Authority allows for appropriate uses and disclosures of protected health information 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 protected health information 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 Department of Defense (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, Personnel, 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 protected health information in order to carry out an activity under the authority of the Commander." See DoD 6025.18-R C7.11.1.2.1.

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

(3) In general, VHA may disclose individually-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 treatment, payment or health care operation purposes. For other purposes not explicitly outlined in this directive, the VA and DoD Memorandum of Understanding (MOU) on Data Sharing outlines the legal authorities for the Departments to share individually-identifiable information under the HIPAA Privacy Rule.

d. **Other Federal Agencies.**

(1) VHA may disclose individually-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 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, and 38 CFR part 46.

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

(4) VHA may disclose individually-identifiable health information, to another Federal agency when legal authority exists to make the disclosures under all applicable federal laws and regulations, (HIPAA, Privacy Act, and 38 U.S.C. 5701, 5705, and 7332). Contact your facility Privacy Officer to determine appropriate legal authority for the disclosure.

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

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

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

27. PUBLIC HEALTH AUTHORITIES

a. **Food and Drug Administration.**

(1) **Routine Reporting.**

(a) VHA may disclose individually-identifiable health information to the Food and Drug Administration (FDA), or a person subject to the jurisdiction of the 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 the FDA,

2. To track products if the person is required to track the product by the FDA,

3. To conduct post-marketing surveillance to comply with requirements of FDA, and/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 cannot disclose information covered by 38 U.S.C. 7332 to the FDA for routine reporting. Such information may be reported to the extent that 7332-protected information is redacted from the information that is being disclosed.

(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 not disclose individually-identifiable information covered by 38 U.S.C. 7332 unless the FDA obtains a court order.

(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. Title 38 U.S.C. 7332(b)(2)(B).

b. **Routine Reporting to State Public Health Authorities.**

(1) VHA may report a patient's individually-identifiable health information, excluding 38 U.S.C. 7332-protected information, to States for public health purposes when there is a signed standing written request letter between the VHA health care facility and the State 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 provide the vaccine or other influenza illness care and documents the care in a medical record system.

(2) VA, as a federal agency, is not required to report any patient information to a State for public health reporting. Under the Federal Supremacy Clause in 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 2013-008, Infectious Disease Reporting, or subsequent policy issue, the Under Secretary for Health requires VHA health care facilities to report infectious diseases to State public health authorities when legally permissible.

(3) A standing written request letter from the State is required and must:

(a) Be in writing,

(b) Specify the public health reporting required and the State law mandating such reporting,

(c) Be signed by a qualified representative of the State agency requesting the information, and

(d) Be valid only for 3 years and then it must be reissued.

(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 medical 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 VHA 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."

c. **HIV Reporting.** 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 pursuant to a standing written request letter. A Federal or State law must require disclosure of the information for a purpose that is authorized by law and a qualified official of the public health authority must make a written request for the information.

d. **Influenza "Flu" Vaccination.**

(1) If a VHA health care facility has an existing signed standing written request letter 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.

(2) In the interests of collaboration with states and in order to provide the best data to the U.S. Centers for Disease Control and Prevention (CDC), the VHA Office of Public Health and Environmental Hazards 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) Influenza vaccination is not mandatory or a condition of employment. Occupational Health cannot send a list of employees who have not or have received the flu vaccination to supervisors. Occupational Health could send vaccination rates to departments as long as the group is large enough that individuals could not be

identified. Occupational Health may not access Veteran/Employee health records. Information should be obtained from the employee directly or per an authorization of the Veteran/Employee.

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 a standing request for ongoing reporting to the State Cancer Registry if continuous reporting is requested. 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 1072, Release of VA Data to State Cancer Registries.

c. **State Prescription Drug Monitoring Programs.**

(1) VHA may disclose individually-identifiable health information to a State Prescription Drug Monitoring Program (SPDMP) without the signed, written authorization of the patient for whom the medication was prescribed. Disclosure may be for the purpose of querying the SPDMP or reporting mandatory prescription information to the State (e.g., batch reporting).

(2) Facility Privacy Officers should work with their health care providers and clinical staff to ensure that a process is in place to track the accounting of disclosures when querying the SPDMP.

(3) A note in CPRS can be used to account for the SPDMP query disclosures; however, the Chief of HIM should be involved in the development of the note template.

d. **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) upon written request when required by law and the request meets the requirements of 38 U.S.C. 5701(f).

29. STATE VETERAN HOMES

a. State Veteran Homes are established by a State to provide nursing home, domiciliary or adult day health care for eligible Veterans. State Veteran's 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 Secretary, Congress and Veterans that State Veterans Homes meet VA standards through an 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, excluding 38 U.S.C. 7332-protected information, to a State Veterans Home for medical treatment or follow-up at the State Veterans Home, if VA is paying a per diem rate to the State Veterans Home for the resident receiving care at such Home and the patient is receiving VA medical care.

c. VHA may disclose 38 U.S.C. 7332-protected information to a State Veterans Home with the signed, written authorization of the individual.

d. If there is no written authorization, VHA may disclose 38 U.S.C. 7332-protected information to the State Veterans Home when a State Veteran Home refers an individual for treatment of 38 U.S.C. 7332 conditions to a VA medical center and the individual returns to the State Veteran Home in order for the State Veterans Home to provide continuity of care and treatment to the resident.

e. State Veteran Home access to the Electronic Health Record (EHR) of a patient will be managed at the facility level. CPRS Read Only will be used to limit access of authorized SVH employees access to a specified claimant's VHA EHR. State Veteran 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 title 38 U.S.C. 7332. The VHA Health Information Access (HIA) office should be contacted for guidance.

30. VETERANS SERVICE ORGANIZATIONS (VSO)

a. VHA may disclose individually-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 Power of Attorney (POA) for Health care (specifying that the POA includes access to the Veteran's health records, using 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 (CAPRI) 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 VHA health care facility's Gains and Losses sheet since there is no authority to disclose this information. Questions from VSOs on this matter need to be forwarded to the facility Privacy Officer.

e. The VHA HIA office should be contacted for CAPRI access by a VSO. VSO employees may be provided with CAPRI read-only access to a specified claimant's VHA EHR, contingent upon the claimant executing a POA or an authorization to release health information, authorizing the VSO unlimited and unrestricted access to all health records, including records protected by 38 U.S.C. 7332.

31. READJUSTMENT COUNSELING SERVICES (RCS) VET CENTERS

a. Vet Centers are part of VHA under the Office of Readjustment Counseling Service. However, the Vet Centers operate separately from VHA health care facilities and are not organizationally aligned within the VHA medical center, VISN, and Chief Network Office (10N) chain of command. Vet Centers report to one of seven Regional Offices and to the VHA Program Office, Readjustment Counseling Service (RCS) program office in Washington, DC.

b. Each Regional Office has a Privacy Officer assigned to those Vet Center within their individual Region to report privacy issues. The VISN or facility Privacy Officers are not responsible for the Vet Centers that are physically located on the VHA property or the ones located near the VHA health care facilities.

c. 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 on the RCS Privacy Policy, contact RCS in VA Central Office in Washington, DC.

32. 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 VHA 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, since 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 (AM&MS), housekeeping, greeting desk/directional desk (no gains and lose sheets), mail room sorting mail but cannot open the mail or deliver mail to individual Veteran rooms.

33. WORK STUDY STUDENTS AND STUDENT VOLUNTEERS

a. Work study students are considered employees for the time during which 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.

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 Voluntary Service Program, and must have written authorization for diagnostic and emergency treatment if injured while volunteering. Student volunteers may not be given electronic access to any individually-identifiable information, such as VistA/CPRS, in the performance of their voluntary duties. Student volunteers may be given verbal or paper individually-identifiable information after the completion of privacy training.

34. 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 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. ***NOTE:*** *See Records Control Schedule (RCS) 10-1 for retention requirements of VHA records.*

(2) VHA must comply with guidelines regarding appropriate uses and disclosures of a deceased individual's protected health information under the HIPAA Privacy Rule for a period of 50 years following the death of the individual.

b. **Deceased Veterans' Information.**

(1) The personal representative of a deceased individual has the same HIPAA Privacy Rule rights as the deceased individual that the personal representative is representing. The personal representatives of a deceased individual 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. Refer to paragraph 5 for more information on personal representatives.

(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 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 34d.).

(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, or

(b) Documentation of the death of such individual, if requested by VHA, and

(c) Representation 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) 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 or other personal representative only for the purpose of obtaining survivorship benefits for the deceased patient's survivor(s). This would include not only VA benefits, but also payments by the Social Security Administration (SSA), Worker's Compensation Boards or Commissions, other Federal, State, or local government agencies, or non-government entities, such as life insurance companies.

(2) 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.

(3) 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.

(4) 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.

(5) Information may only be disclosed outside VHA for research purposes pursuant to the research provisions, see paragraph 13, of this directive.

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 overrides the HIPAA Privacy Rule in regard to family members obtaining a deceased Veterans' records. 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).*

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 VHA medical facility Director determines that such disclosure is necessary for the survivor to receive 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 the 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 the next-of-kin.

(4) If there is any indication that the requested information will be used in a lawsuit, the Regional Counsel must be informed promptly of the circumstances. No further actions can be taken without guidance from the Regional Counsel.

35. VHA SYSTEMS OF RECORDS

a. Information concerning an individual will not be collected or maintained in such a manner that information is retrieved by an individual identifier, unless a system notice is first published in the Federal Register. Without prior publication of a system of records notice, such a system would be an illegal system of records and the personnel operating it would 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.

b. Prior to collecting or maintaining information concerning an individual in what would be a system of records, the VHA health care facility must verify the existence of a published system of records notice. If it is determined that a published system of records notice does not exist, contact the VHA Privacy Office for assistance prior to any collection of information. ***NOTE:*** *Contact the VHA Privacy Office if assistance in this determination is needed.*

c. Prior to collecting information from an individual, the VHA health care facility needs to ensure compliance with the Paperwork Reduction Act and 5 CFR part 1320, Controlling Paperwork Burdens on the Public.

d. Records are not to be established and information collected until the system of records is approved by the Secretary of Veterans Affairs, published for public comment in the Federal Register, and appropriate reports are submitted to the Office of Management and Budget (OMB) and to Congress.

e. Components of a system of records notice includes:

(1) System Location - Specifically identify each address or location where records are maintained (e.g., Records are maintained at the VA medical center, field office, Vet Center, or warehouses, etc.).

(2) Categories of Individuals in System - Identify each category of individuals covered by the system (e.g., Veterans and their family members, members of the Armed Services, former employers, contractors, etc.).

(3) Categories of Records in System - Identify each category of records covered by the system. This must be an all-inclusive list (e.g., health record, administrative record, subsidiary records, etc.).

(4) Purpose - Describe the purposes for which VA intends to use information in the system. (e.g., Information in this system of records is used to verify the household income of certain Veterans receiving VHA health care benefits, etc.).

(5) Routine Uses - These are brief, concise, clear statements of the possible reasons for disclosures of the information maintained in the systems of records. A routine use must be published in the Federal Register at least 30 days before a disclosure may be made pursuant to the routine use.

(6) Storage - Specifically describe the medium or manner in which the records are maintained, such as microfilm, magnetic tape, floppy disk, or paper file folders.

(7) Retrievability - Describe how the records are indexed and retrieved.

(8) Safeguards - Briefly describe measures taken to prevent unauthorized access and disclosure of records, such as physical security, personnel screening or technical safeguards.

(9) Retention and Disposal - Describe how long the records are maintained and how VA disposes of them.

(10) Notification, Contesting, & Record Access Procedures - Provide the address(es) of the VA Office(s) to which inquiries should be sent and provide name(s) and address(es) of the VA office(s) to which the individual may go or write to obtain information from his/her record. ***NOTE:*** *For additional information on Systems of Records or if you think you may be establishing a new system of records, contact the facility Privacy Officer.*

f. 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 VHA health care facility that are covered by a VHA system of records notice are in the system of records "Patient Medical Records-VA", 24VA10P2. For a list of all VHA systems of records notices, go to: http://vaww.vhaco.va.gov/privacy/SystemofRecords.htm. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

36. RELEASE FROM NON-VHA SYSTEMS OF RECORDS

a. Within VHA health care facilities, several non-VHA systems of records are subject to the provisions of the Privacy Act of 1974, VA Confidentiality Statutes or the HIPAA Privacy Rule. Non-VHA systems of records include, but are not limited to, Official Personnel Folders (OPF), Employee Health Records, and VA Police Records.

b. If, for example, a VHA employee produces a health record in support of a patient's claim for VA disability benefits, this health record is technically under the authority of the local VBA Regional Office. If your facility has VA benefits health information such as Compensation and Pension exams, refer to your facility Privacy Officer for disclosure guidance.

c. Questions regarding right of access, amendment or release of non-VHA records/information should 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.

d. VHA health care facility Privacy Officers should 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 VHA facility.*

37. 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 protected health information 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 protected health information for the following purposes in the administration of educational programs, quality assurance activities and other assessment such as:

(a) To assess the competency of trainees and staff;

(b) To assess the number and types of patients from which trainees learn, or that staff members care for;

(c) To comply with clinical or education accreditation standards;

(d) For academic or disciplinary actions involving trainees or staff for which individually-identifiable health information is relevant; and

(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 trainees or faculty members, copies of that data that has been disclosed becomes the property of the Affiliated Educational Institutions and is no longer considered a 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 individually-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 business associate agreement.

(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, etc.) to the extent that the information is relevant to their review pursuant to a business associate agreement.

(2) Individuals who conduct an audit or evaluation and receive or review individually-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 individually-identifiable information in facility operations, including during the check-in process.

(2) Employees must exercise appropriate precautions and safeguards when discussing Veterans' individually-identifiable information in public areas, such as clinic waiting rooms. Appropriate safeguards for auditory privacy include:

(a) Using the Veterans Health Identification Card (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 of SSN 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”, and

(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 VHA 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 should be placed as far from the reception desk as possible.

(5) Check-in kiosks should have privacy screens and be placed in a manner that individuals in the waiting area or walking past cannot see what individually-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 clinical residents must not include any unique identifiers before disclosure. Only non-identifiable information, which has the Unique Identifiers removed, may be provided. A Business Associate Agreement and Data Use Agreement are not required with the Certification Board.

(2) VA providers maintaining a listing of Veteran’s individually-identifiable information for submission of non-identifiable information to their Certification Boards must safeguard this individually-identifiable information on a shared network drive and not on a physical log.

e. **Claims Folder (VBA).**

(1) Requests for release of medical or health information in Veterans' claims folders should 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 VHA health care facility in accordance with this directive. ***NOTE:*** *VBA and VHA are in the process of modifying the applicable Privacy Act systems of records covering the C&P exams. Once these modifications are made, this policy may no longer be applicable.*

(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 system of records, even though the HINQ request is not maintained after the information is placed within VistA. 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 system of records, "Health care Provider Credentialing and Privileging Records-VA" (77VA10Q).

(2) Requests for VHA provider credentialing and privileging information or records need to be processed in accordance with VHA Handbook 1100.19, Credentialing and Privileging, Privacy Act, FOIA, and the provisions of this directive.

(a) Requests from VHA providers for copies of their individual records maintained in their Credentialing and Privileging folder (77VA10Q), will be processed as a first party right of access.

(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 prior to disclosure.

(3) Each privileged health care provider must have a Credentialing and Privileging file established electronically in VetPro, with any paper documents maintained according to the requirements of the standardized folder. Other credentialed health care providers may have a credential file maintained in the same system of records even though they may not be granted clinical privileges.

g. **Federal Parent Locator Service.**

(1) The Department of Health and Human Services (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 VHA health care facilities directly for address information on absent parents. Any requests received by VHA health care facilities for assistance in locating an absent parent must be returned to the requesting agency and the requester should 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

h. **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, or

(d) A Veteran may hear a conversation that a provider is having with another patient while waiting to be seen in the Emergency Room 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 as long as you do not identify them as a patient or link the individual with an appointment or potential health information;

(d) Using VHIC for identification of the patient; or

(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 areas 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/resident/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 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/resident/nurse initials; acuity (a number from 1-5); number of unverified orders; number of active orders/number of completed orders; and elapsed minutes. Patient 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 facility Privacy Officer.

(6) When posting treatment guidelines in a patient's room, the titles should 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.

i. **Medical Opinions/Forms Completion.**

(1) VHA 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 CFR 17.38 and VHA Directive 2008-071, Provision of Medical Statements and Completion of Forms by VA Health care Providers, or subsequent policy issue). VHA health care providers may provide these forms directly to the patient. However, if the VHA health care provider is asked to provide the form directly to a third party, such as an employer or benefits agency, the VHA health care provider must 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 VHA health care providers regarding the individual's medical conditions and/or opinions for submission in support of a claim for VA benefits.

(b) In response to such a request, VHA health care providers must provide a statement or opinion describing the patient's medical condition, prognosis and degree of function.

(c) When the 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, etc.), the Veteran must sign VA Form 10-5345, Request for and

Authorization to Release Medical Record or Health Information, prior to the disclosure being made.

(3) Medical Opinions for Non-VA Purposes.

(a) Individuals may also ask VHA health care professionals for opinions to assist them in filing claims with other agencies. For example, Family Medical Leave Act forms, life insurance application forms, non-VA disability retirement forms, State workman's compensation forms, and state driver's license or handicap parking forms.

(b) These opinions may be provided in the same manner and under the same restrictions as opinions furnished for VBA claim purposes.

j. **Release of Name and/or Address (RONA).**

(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 CFR 1.576(b)), 38 U.S.C. 5701, and the HIPAA Privacy Rule).

(2) Any organization that wants to receive a list of names and addresses of present or former patients and their dependents must make written application under the provisions of 38 CFR 1.519 and VA Handbook 6300.6, Procedures for Releasing Lists of Veterans' and Dependents' Names and Addresses, to the Director, Privacy and Records Management Service (005R1A) 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 CFR 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 CFR 1.518(c)). Letters for the purpose of debt collection, canvassing, or harassing a patient will not be forwarded.

k. **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, Request for and Authorization to Release Medical Records or Health Information. 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 VHA health care facility Public Affairs Office and the Public Affairs Guidelines will be 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 CFR 164.512(j)(1)(i). This information would 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 his medicine immediately. No other individually-identifiable information may be given. VHA may not, except as stated above, disclose diagnoses or other health information to the news media.

(5) **Employee Interviews.** The employee must obtain the appropriate approval in accordance with Public Affairs policy to speak to the news media. Employees would not be authorized to disclose any individually-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.*

l. **ROI from Outside Sources.**

(1) Private hospital or health care provider records that have been incorporated into the individual's health records are considered part of the VHA records and are subject to the disclosure provisions of the Privacy Act, the HIPAA Privacy Rule, 38 U.S.C. Section 5701 and 7332, and FOIA.

(2) An individual requesting this type of record should be encouraged to obtain the information from the hospital or health care provider's office that is the original source of the information. However, if the individual insists on obtaining a copy from VHA, the request should be processed under the policies in this directive.

(3) Requests for information in the record that originated with another Federal agency must be referred to the agency that created the documents. The individual 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. Information from health records of beneficiaries of other Federal agencies and allied governments treated or examined in VHA health care facilities can only be released under paragraph 27 of this directive.

m. **Producing and Using Photographs, Digital Images or Video and/or Audio Recordings.**

(1) VHA intending to produce and use photographs, digital images, or video or audio recordings for official purposes must obtain the consent of persons whose personally identifiable image, likeness, or recording will appear or be heard in such products using VA Form 10-3203, Consent for Production and Use of Verbal or Written Statements, Photographs, Digital Images, and/or Video or Audio Recordings by VA, before producing any photograph, digital image, or video or audio.

(2) VHA must obtain an authorization from the patient or personal representative using VA Form 10-5345, Request for and Authorization to Release Medical Records or Health Information, prior to disclosing for official purposes a photograph, digital image, or video or audio recording if the product contains individually identifiable health information or protected health information.

(3) Refer to VHA Directive 1078, Privacy of Persons Regarding Photographs Digital Images and Video or Audio Recordings, for additional guidance.

n. **Veteran Identification and Designation of Treatment Areas.**

(1) A VHA 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 VHA 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 pajamas, robes, wrist bands, etc., that are different from other patients and which would identify them to VHA 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. 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 hospital rooms.

o. **Virtual Lifetime Electronic Record.**

(1) In April 2009, President Obama directed the VA and DoD to lead the efforts in creating the Virtual Lifetime Electronic Record (VLER), 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." Implementation and access to VLER is a VA-DoD interagency initiative that will provide a simple, cost-effective means for electronically sharing relevant health and benefits data of Veterans and Servicemembers.

(2) VLER utilizes the eHealth Exchange (formerly Nationwide Health Information Network (NwHIN)) 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; only requested information is exchanged via a virtual architecture.

(3) The participating health care providers will have a "view only" option to see the Veteran's information once the Veteran has completed an authorization (VA Form 10-0485, Request for and Authorization to Release Protected Health Information to eHealth Exchange). Once a patient completes the form, the patient is then "opted-in" for sharing of their health information.

NOTE: *For additional information about VLER and the eHealth Exchange, go to: http://www.va.gov/vler/.*

38. GENERAL OPERATIONAL PRIVACY REQUIREMENTS

a. **Designation of Privacy Officer.**

(1) VHA must retain a full-time Privacy Officer.

(2) Each VHA health care facility Director must designate at least one facility Privacy Officer who reports directly to the VHA health care facility Director, Associate Director, or Assistant Director and one alternate Privacy officer who may or may not report to the Triad. The facility FOIA Officer and the facility Privacy Officer may be the same person.

(3) Each VHA Central Office program office should have a designated Privacy Liaison to coordinate privacy activities of their program office with the VHA Privacy Office.

b. **Management of Release of Veteran Information.**

(1) Release of information from the Veteran's health record is a complex function, requiring trained and qualified employees and expert guidance. The management function should be assigned to the facility Chief, HIM or to the facility Privacy Officer.

(2) Release of information must provide for the timely release of information to written requests for information received by VHA. Release of Information staff must use the ROI Plus software to track the accounting of disclosures. To ensure timely and informed release of information it is recommended that all requests be processed through a central point.

(3) The facility Privacy Officer must monitor the disclosure of individually-identifiable health information through random spot-checks which are to be conducted quarterly.

(4) The Chief, HIM or facility Privacy Officer must monitor the Turn-Around Report (TAT) from the ROI Plus software to identify backlogs and expedite responses to requests for information. For instructions for running the TAT Report, see the ROI Plus Administrative Manual located at http://vaww.vhaco.va.gov/privacy/ROI.htm. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

(5) The Regional 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) Individuals 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 VHA health care facility Privacy Officer, or designee, or the VHA Privacy Office (10P2C1), 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 VHA health care facility Privacy Officer, or designee, or the VHA Privacy Office should obtain mailing information in order to send the privacy complainant the Notice. The Notice should be mailed out within 10 business days if the Notice is not given in person. A cover letter should be included when the Notice is mailed.

(4) All privacy complaints, regardless of validity, must be:

(a) Documented in the Privacy and Security Event Tracking System (PSETS) within one hour of receiving the notification,

(b) Communicated to leadership, as appropriate (Director, VISN, VHA Privacy Office, Office of Inspector General, Office of General Counsel),

(c) Investigated promptly and documented in PSETS, and a file should be kept to include interviews of involved parties and reports of contact requested, as outlined in paragraph 38.d.,

(d) Documented outcomes of the investigation should be provided to the VHA supervisor and coordinated with stakeholders (i.e., Human Resources for sanctions or disciplinary actions, union representatives, department heads),

(e) Managed to full resolution and closure upon notification from the Data Breach Response Service (DBRS) in PSETS, and

(f) If a complaint is found to be valid by the Privacy Officer (e.g., violation of privacy policy) the ticket status under PSETS must be changed from a complaint to an incident.

(5) VHA health care facility Privacy Officers should trend the types of privacy complaints identified and report these trends to the facility leadership bi-annually and VHA Privacy Office, upon request.

(6) All privacy complaints, regardless of validity, are audited in accordance with VA Directive 6502, VA Enterprise Privacy Program, and VA Handbook 6502.1, Privacy Event Tracking.

(7) A written response must be provided to the privacy complainant as soon as possible or no later than 60 working days, explaining the results of the investigation for all privacy complaints.

(8) When the privacy complaint alleges unauthorized access and you cannot prove that the access is likely, or more likely than not, authorized, the access must be presumed to be unauthorized.

(9) When an individual requests their Sensitive Patient Access Report (SPAR) and does not give a period of time for the running of the report, the VHA health care facility Privacy Officer should ask the individual for the timeframe desired. If the individual wants the SPAR for the entire timeframe for which it exists, then it would be provided as such under Right of Access.

(10) The VHA Privacy Office serves as the central authority for coordination of Department of Health and Human Services (HHS) Office for Civil Rights (OCR) privacy and security complaints received by all VHA health care facilities. Any HHS-OCR privacy or security complaints received by VHA health care facilities should be forwarded to the VHA Privacy Office. If the facility Privacy Officer receives a HHS-OCR notification letter, this notification letter should be forwarded via encrypted Email to VHAPrivIssues@va.gov.

(11) VHA may not retaliate against a person for exercising rights provided by the HIPAA Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates these provisions. VHA may not require an individual to waive any right under these provisions as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

(12) An individual has 3 years from the date of the privacy violation or concern to file a privacy complaint with VHA unless good cause to extend timeframe is shown. The Department of Health and Human Services (HHS), Office for Civil Rights (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 CFR 160.306).

d. **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 should be 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 should 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 should 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 should contain a brief summary of the interview including general information about the interviewee(s) and their responses.

(d) Privacy Officer's official recommendations to HR and 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 where contacted by the Privacy Officer. This may include facility ISO, VA Police and Security, Office of Regional Counsel, etc.

(f) Copies of the signed final complaint response letters and correspondence with the complainant and affected individuals.

(g) If a privacy complaint is valid and determined to be a privacy violation, the PSETS ticket should be changed to an Incident. A copy of the PSETS ticket and determination of the VA DBRS and Data Breach Core Team (DBCT) should be kept with the complaint file. If the DBCT determines the privacy violation to be a data breach as outlined in VA Handbook 6502.1, 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 Privacy Officer as a result of sending notification or credit monitoring letters as required by VA Handbook 6502.1 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, XLIII-8 and XLIII-9.

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 the VA Office of Inspector General (OIG), Office of Special Counsel (OSC), or Congress, it does not free VA employees from their obligation to safeguard individually-identifiable information, including protected health information (PHI), to the extent it is protected from disclosure.

(2) A whistleblower, which is a member of the VA workforce or VHA business associate, who reasonably 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 protected health information 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 protected health information, except information protected by 38 U.S.C. 7332 (HIV, Sickle Cell, Drug and Alcohol Treatment) to OSC, a public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of VHA, 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.

(4) An employee who discloses protected health information to an entity other than those listed above may be considered to have made an unauthorized disclosure in violation of the Privacy Act, 38 U.S.C. 7332, HIPAA Privacy Rule or VHA policy. Such unauthorized disclosure may result in disciplinary action.

(5) Whistleblower retaliation will not be 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.

(6) If VHA receives a privacy complaint that an employee disclosed information under a potential whistleblower activity, consult HRMS, Regional Counsel or VHA Privacy Office to determine whether privacy legal authority existed for the disclosure.

f. **Faxes.**

(1) Information on drug, alcohol, HIV, or sickle cell anemia status may not be transmitted by fax machine, unless the transmittal is directed to medical personnel to the extent necessary to meet a bona fide medical emergency.

(2) 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.

(3) Fax machine transmittals may also be used for non-patient care, however, all established fax protocols must be strictly observed.

(4) 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."

(5) 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: *See VHA Handbook 1907.01, Health Information Management and Health Records, and VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program, for additional information.*

g. **Email.**

(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 (PII) or protected health information, unless the data is encrypted using public key infrastructure (PKI) or Rights Management Services (RMS).

(3) Communication with Veterans via Email may occur if it is for marketing purposes and no reply is utilized. Administrative personnel may communicate with Veterans as long as PHI is not being shared. Researchers must have IRB approval prior to Email communication with Veterans. Provider-Veteran communication for any other purposes must use secure messaging through MyHealtheVet.

(4) Last 4 of SSN. VA OGC has determined that the last four digits of SSN and first initial of the last name is not a unique identifier of a single individual by itself. However, if any other individually-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 Outlook Email without encryption.

(5) Subject Line. The first initial and last four digits of the SSN by itself can be included in the subject line of an Email message but only if no other identifying information is contained within the body. Only non-identifiable information can be placed in the subject line.

(6) Outlook Calendar. It is not acceptable to include PHI in the Microsoft Outlook Calendar. The Outlook Calendar may be placed on a Shared Drive with protected health information 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) Outlook Instant Messaging (IM). PHI should not be shared, stored or retrieved using MS Outlook, Microsoft Lync. This is not a viable option as there are other venues for PHI to be stored, shared, and retrieved such as CPRS and VistA.

h. **Training of Personnel.**

(1) 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.

(2) Newly hired personnel must complete privacy training within 30 days of employment. If personnel have access to protected health information, they are required to take the Privacy and HIPAA Focused training.

(3) If personnel 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.

(4) If personnel do not have access to VA computer systems or direct access to protected health information they can take the VA Privacy Training for Personnel without Access to VA Computer Systems. This training is available in the Talent Management System (TMS).

(5) At a minimum, instruction must be provided within 6 months of significant change in Federal law, regulation, this policy, or facility or office procedures.

(6) VHA health care facilities must work in collaboration with TMS to track completion of privacy training.

(7) Contractors with access to protected health information must complete Privacy and HIPAA training if their training does not comply with VHA privacy policy requirements.

(8) VA Handbook 6500 outlines the consequences if a user does not engage in or cannot meet general or specialized training requirements.

i. **Contracts.**

(1) All contracts must meet contracting requirements as dictated by VA's Office of Acquisition and Material Management and the Federal Acquisitions Regulations (FAR).

(2) Any contract between VHA and a contractor for the design, development, operation, or maintenance of a VHA system of records or any contract that necessitates the use of individually-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. See Health Information Access (HIA) Web site for additional information on business associates: http://vaww.vhadataportal.med.va.gov/. ***NOTE:*** *This is an internal VA Web site that is not available to the public.*

(4) Business associates must follow VHA Handbook 1605.05, Business Associate Agreements.

(5) All contractors and business associates must receive privacy training annually.

(a) For contractors and business associates who do not have access to protected health information in VHA computer systems, such as VistAWeb or CPRS, 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 protected health information in VHA computer systems, such as VistAWeb or CPRS, this requirement is met by receiving the Privacy and HIPAA Focused 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, Appendix A, Contract Security, checklist, to determine if there is VA sensitive information and if a Business Associate Agreement (BAA) is needed. The facility Privacy Officer must work collaboratively with the Information Security Officer and Contracting Officer to ensure the checklist is completed accurately and timely. The facility Privacy Officer should not sign a blank checklist nor should they be the subject matter expert for the checklist.

(7) The facility Privacy Officer must determine what privacy requirements under VA Handbook 6500.6, Appendix C, are required for the contract.

j. **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.*

NOTE: *In the event a VHA 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 individually-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.

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. A qualified biostatistician (a biostatistician with a master's or Ph.D degree) 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.

b. 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 Title 38 United States Code (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.

(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 social security numbers is <u>not</u> 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 social security number (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 social security number. 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 Web site 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 File 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
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	OPM/	OPM	Office of	Title 5

System Name	*System Number*	*System Manager*	*Responsible Office*	*Types of Records*
Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers	GOVT-3		Personnel and Labor Relations	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
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