PRIVACY POLICY

MCP 001-31

Veterans Health Care System of the Ozarks (VHSO)
Fayetteville, AR 72703

Rescinded Document:
001-31, Privacy Policy, dated February 26, 2018

Signatory Authority:
Medical Center Director

Effective Date:
February 7, 2023

Responsible Owner:
Privacy Officer

Recertification Date:
February 7, 2028

1. POLICY

This Veterans Healthcare System of The Ozarks (VHSO) policy will develop, implement, maintain, and enforce a structured privacy program to properly use, disclose and safeguard individually identifiable information. The privacy program is designed to allow continued operation of mission-critical activities while ensuring the integrity, availability, confidentiality, and authenticity of data and information; minimum necessary access to protected health information; and a continuing awareness of the need for, and the importance of, information privacy within the facility.

2. JUSTIFICATION

All members of the workforce are responsible for complying with this privacy policy, applicable federal laws, and regulations, VA/VHA policies, as well as the procedures and practices developed in support of these policies. All facility privacy policies and procedures must be consistent with VHA 1605 Directives and Handbooks.

3. RESPONSIBILITIES

a. **Medical Center Director or Designee.** The Medical Center Director (MCD) is responsible for:

(1) Providing the necessary resources (funding and personnel) to support thePrivacy Program, maintaining a culture of privacy, and ensuring that the facility meets all the privacy requirements mandated by VA/VHA policy and other federal legislation [e.g., Freedom of Information Act (FOIA) [5 U.S.C.§ 552], Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule [45 C.F.R. Parts 160 and 164], Health Information Technology for Economic and Clinical Health (HITECH) Act, Privacy Act (PA) [5 U.S.C. §552a], VA Claims Confidentiality Statute [38 U.S.C. 5701], Confidentiality of Medical Quality Assurance Review Records [38 U.S.C. 5705], and Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Medical Records [38 U.S.C. §7332].

(2) Ensuring that the facility meets all the privacy requirements mandated by VA/VHA policy and other federal legislation ensuring compliance within the facility with all Federal Laws, regulations, VA regulations and policies, and VHA policies relating to privacy.

(3) Ensuring Privacy Officer coverage for the facility and its associated clinics. It is required by VHA Privacy Policy that the facility Privacy Officer report directly to the Medical Center Director, Associate Director or senior individual who reports directly to and is supervised by the Medical Center Director and whose primary responsibilities at the facility include privacy program compliance. Providing coverage for off-hours operations (24/7) when the facility PO oralternate is not available.

(4) Ensuring facility Privacy Officer is fully involved in all projects concerning the access, collection, maintenance, use and/or disclosure, transmission, amendment and/or disposal of individually identifiable information (III).

(5) Ensuring that new and revised Memorandums of Understanding (MOU), Contracts, Data Use Agreements (DUA), BAA, or similar agreements which involve the collection, transmission, use or sharing of information are reviewed by the facility Privacy Officer, in accordance with VA Handbook 6500.6, Contract Security, prior to approval by ExecutiveLeadership.

(6) Ensuring that the facility Privacy Officer is included in discussions regarding privacy concerns of the facility which are addressed in strategic initiatives and maintains afacility culture of privacy.

(7) Cooperating with the facility Privacy Officer in any investigation, mediation strategies, or correspondence that is required to investigate and resolve a complaint or allegation and ensuring that appropriate disciplinary action is taken.

(8) Annually certifying (or on an as needed basis), to the VHA Privacy Office, that privacy training has been completed for all personnel. This shall include all employees, volunteers, contractors, students, residents, and any other person performing or conducting services on behalf of the facility.

(9) Fully cooperating in submissions of Facility Self-Assessments (FSA) and on-site Privacy Compliance Assurance Assessments as required by the Privacy Compliance Assurance (PCA) Office.

(10) Ensuring that signs are placed alerting Veterans to auditory privacy concerns in areas, elevators, and other spaces requiring auditory privacy and that facility employees exercise appropriate precautions and safeguards when discussing Veterans III in public areas, such as clinic waiting rooms.

b. **Privacy Officer (or designee).** The Privacy Officer (PO) is responsible for:

(1) Developing, implementing, and updating local privacy policies and procedures.

(2) Reviewing all health care center facility policies to ensure compliance with all privacy laws and regulations.

(3) Conducting periodic physical assessments, compliance reviews and/or audits of the facility's collection, use, storage and maintenance of personal information. Reviews will include identification and correction of privacy vulnerabilities related to incidental disclosure such as posted and displayed PHI in clinical areas.

(4) Establishing effective working relationships with the Information Systems Security Officer (ISSO), Facility Chief, Information Officer (FCIO), Contracting Officer, Compliance Officer, Research Compliance Officer, and Human Resources Management (HRM) personnel to ensure that local policies and procedures which mayimpact the privacy program support and complement each other.

(5) Ensuring that Executive Leadership is apprised of all privacy vulnerabilities and related issues.

(6) Coordinating with the Information System Security Officer (ISSO) for the assurance of reasonable safeguards asrequired by the HIPAA Privacy Rule, HITECH or other federal privacy statutes.

(7) Serving as the facility's point of contact (POC) for privacy matters relating to privacy policies and procedures.

(8) Ensuring that all workforce members (employees, volunteers, students and contractors) complete mandatory privacy training, in conjunction with the facility Education Coordinator and other staff/office, per facility policy, and review training records as per Appendix D in VHA Directive 1605.03(1).

(9) Ensuring members of the workforce know whom to contact when a privacy complaint or incident is identified or received.

(10) Monitoring facility and workforce compliance with VHA privacy policies and procedures as well as compliance with local privacy policies and procedures.

(11) Identifying and reviewing areas within the facility for auditory privacy risks, to ensure appropriate safeguards are in place to limit incidental disclosures. Ensure the placement of signs alerting Veterans and staff to auditory privacy concerns in the waiting areas, elevators, and other spaces requiring auditory privacy and ensure the placement of chairs in waiting areas are optimally placed to minimize auditory privacy violations.

(12) Ensuring the placement of signs prohibiting the use of camera phone or video in restricted areas to comply with VHA Directive 1078(1).

(13) Ensuring processes are in place for the appropriate accounting of disclosures of individually identifiable information made by the facility and appropriate utilization of the Release of Information (ROI) Plus software or other tracking mechanism are used in

accordance with facility's policies and procedures. The processes will include accounting for authorizations electronically conducted through iMedConsent™.

(14) Collaborating with various program officials, and the Contracting Officer, to ensure identification of all entities meeting the definition of Business Associates.

(15) Maintaining a list of active Business Associates utilized by the facility and ensuring all Business Associates have a signed BAA in place prior to disclosure of individually identifiable health information (IIHI) and that the Business Associate adheres to the requirements of the BAA.

(16) Collaborating with the facility Records Manager to ensure that RCS 10-1 is followed for record control requirements and no unauthorized system of records are being kept.

(17) Ensuring all facility developed paper, web-based or electronic forms that collect personal information contain the appropriate Privacy Act statements.

(18) Reviewing and approving all Memorandum of Understanding (MOU), contracts, and DUAs when required for the sharing of VA sensitive data between the facility and other parties.

(19) Ensuring prompt investigation and follow-up on allegations or known occurrences of privacy violations or, complaints including logging the complaint or violation in the Privacy and Security Event Tracking System (PSETS). PSETS should be initiated upon notification of the violation or complaint during normal business hours or as soon as possible outside of normal business hours. If a privacy violation presents the risk of media involvement, congressional inquiry, legal action, immediate harm to any individual or any other high-risk outcome, the incident must be reported within one hour of discovery regardless of discovery time (even during non-business hours).

(20) Promptly reporting any potential privacy complaint, allegation, or activity thathas VISN-level or national-level significance to the VHA Privacy Office.

(21) As a non-voting member of the facility Institutional Review Board (IRB), the PO will review all human subject research protocols, exempt and non-exempt, in accordance with VHA Directive 1200.5(01) and other applicable guidance to ensure legal authority exists prior to use and disclosure of VHA information for research.

(22) Collaborating with the facility Information System Security Officer (ISSO), Facility Chief Information Owner (FCIO) to ensure that a Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) are completed on all information technology systems,applications or programs that collect, maintain, and/or disseminate personally identifiable information (PII).

(23) Reviewing, processing, and monitoring requests to amend any information or record retrieved by an individual's name that is contained in a VA system of records, to

include designated record sets, and coordinating such requests with the author of the document.

(24) Collaborating with the facility Information System Security Officer (ISSO), Contracting Officer Representative (COR) and the Contracting Officer to ensure all contracts are reviewed in compliance with VA Handbook 6500.6.

(25) Ensuring all facility policies and procedures relating to HIPAA, HITECH, PA, 38 U.S.C. § 5701, § 5705, and § 7332, and FOIA are consistent with current guidelines and requirements, complementing and supporting each other. Ensuring local departmental policies and procedures are developed if not specifically outlined in the facility privacy and FOIA policies.

(26) Ensuring local departmental policies and procedures are developed if not specifically outlined in the facility Privacy policy.

(27) Provide awareness training through various means for Veterans to inform them of their privacy rights and responsibilities.

(28) Completing and submitting the Privacy Facility Self-Assessment (FSA) by the last business day of each quarter or as required by PCA and work with facility staff and leadership to facilitate a successful Privacy Compliance Audit.

(29) Ensuring that the Social Security number (SSN) usage is reviewed to determine the necessity and encouraging the reduction of the usage of the SSN whenever possible.

(30) Administering facility C3R activities, documenting the findings of these activities, remediating non-compliance, recording actions taken and making the documentation of these actions available to PCA upon request. ***NOTE:*** *This requires that all C3R activities are appropriately documented. C3R tools and checklists on the PCA intranet site or other tools generated by the facility may be used to ensure documentation.*

c. **FOIA Officer.** The FOIA Officer is responsible for:

(1) Processing all FOIA requests (for Federal records that would not otherwise be disclosed in accordance with HIPAA or the PA) that are traditional FOIA requests. Ensuring all FOIA requests or HIPAA/PA requests where information is withheld under a FOIA exemption is entered into FOIAXpress® within the same day as receipt.

(2) Requests on deceased Veterans by the legal next of kin or personal representative of the estate that have been determined to be a full disclosure of the records is no longer processed under FOIA. Since they are no longer processed under FOIA, they do not require entry into FOIAXpress®. Medical records requests by legal next of kin or personal representative of the estate involving 38 U.S.C. § 7332 information is required to obtain survivorship benefits. If the 38 U.S.C.§ 7332 information is required, 38 U.S.C. § 7332 will be disclosed pursuant to the statute. In

such instances, requests are not processed under the FOIA and therefore do notrequire entry into FOIAXpress®.

(3) Medical records requests by the legal next of kin or the personal representative of the estate in which involve 38 U.S.C. § 7332 information and a determination has been made that the 38 U.S.C. 7332 information is not required to obtain survivorship benefits, will be processed as FOIA requests. In these instances, the 38 U.S.C. § 7332 information will be withheld citing FOIA Exemption 6 and Exemption 3. This guidance has not changed from previous direction.

(4) Third Party medical record requests that are accompanied with a HIPAA-compliant written authorization by the legal next of kin or the personal representative of the estate that do not involve 38 U.S.C. § 7332 information and to which a full disclosure will be made are no longer processed under the FOIA. Since these requests are no longer processed under the FOIA, they do not require entry into FOIAXpress®.

(5) Third Party PA requests that are accompanied with a HIPAA-compliant written authorization, but the authorization does not address 38 U.S.C. § 7332 protected information is no longer processed under the FOIA. Privacy/FOIA Officers and Health Information Management (HIM) staff should make efforts to confirm the individual does not wish the 38 U.S.C. § 7332 protected information disclosed. If this was an oversight by the individual, a new authorization must be obtained before the information may be disclosed. If the individual does not wish the 38 U.S.C. § 7332 protected information disclosed, the information must be redacted if possible. If adequate redaction is not possible, the record must be withheld in its entirety. In this instance, the redaction is not pursuant to the FOIA. The information is redacted without citing a FOIA exemption. Since these requests are no longer processed under the FOIA, they do not require entry into FOIAXpress®.

(6) Third Party PA requests that are not accompanied with a HIPAA-compliant written authorization, the Privacy/FOIA Officers and HIM staff should make every effort to obtain a valid authorization on these requests. If the facility is unable to obtain an authorization, these requests will be processed under the FOIA. As FOIA requests, these requests will be closed withholding the medical record in its entirety citing FOIA Exemption 6 and Exemption 3 citing 38 U.S.C.§ 5701. As FOIA requests, these requests must be entered into FOIAXpress®.

(7) Other responsibilities as defined by VHA FOIA Office.

d. **Information Security Officer (ISSO) or designee.** The ISSO is responsible for:

(1) Coordinating with the facility PO for the assurance of reasonable safeguards as required by the HIPAA Privacy Rule, HITECH or other federal privacy statutes.

(2) Coordinating, facilitating, and updating the establishment of information security policies and procedures, to work in tandem with privacy policies and procedures. Serving as the facility's point of contact for matters relating to the information security policies and procedures.

(3) Establishing effective working relationships with the PO; FCIO; Contracting Officer; Compliance Officer; Research Compliance Officer, and HRM personnel to assure that information technology (IT) security and HIPAA/FOIA/PA/Federal Information Security Management Act (FISMA) policies and procedures complementand support each other.

(4) Reviewing and evaluating the security program impact(s) of any proposed facility information privacy policy and procedure changes.

(5) Collaborating with the facility PO on addressing/resolving privacy complaints, investigations, and access rights to audits and other information maintained by the ISSO, on issues related to common facility impacts from privacy and security requirements.

(6) Collaborating with the facility Privacy Officer, Area Manager and System Owner to ensure that the Privacy Threshold Analysis (PTA) and the Privacy Impact Assessment (PIA) if applicable, are completed and fully executed on all information technology systems, applications or programs that collect, maintain and/or disseminate PII.

(7) Entering all Information Security violations through the Privacy and Security Event Tracking System (PSETS) to the VA Cyber Security Operations Center (VA-CSOC) within 1 hour of discovery.

(8) Ensuring that all media (paper, electronic, CDs, disks, portable devices, etc.) with III is disposed of via approved means.

(9) Ensuring that Executive Leadership is apprised of all information security related issues.

e. **Clinical Service Chiefs (or designee(s) and Appropriate Staff.**

(1) Reviewing and determining appropriateness for granting individuals' requests for record amendment.

(2) Accessing, using and disclosing protected health information only when legal authority exists.

f. **Area Manager/Facility Chief Information Officer (FCIO) or Designee.** The FCIO is responsible for:

(1) Coordinating with facility ISSO and PO to provide technical advice and other assistance relative to the reasonable safeguards requirements of privacy statutes and regulations dealing with implementation of IT systems, policies, and procedures.

(2) Identifying each locally maintained computer system that contains III and providing technical input for various mandated documents, reports, and investigations.

(3) Ensuring all computer rooms meet acceptable reasonable safeguards and that minimum necessary access is maintained.

(4) Collaborating with the ISSO, PO and Information System Owner to ensure that the PTA and the PIA, if applicable, are completed and fully executed on all information technology systems, application or programs that collect, maintain and /or disseminate PII.

g. **Chief, Human Resources Management (HRMS) or designee.** The Chief, Human Resources Management (HRM) is responsible for:

(1) Providing consistent and uniform guidance to supervisors and managers regarding personnel actions, sanctions, or other actions to be taken when employees have violated information privacy practices, laws, regulations, policies and procedures, and rules of behavior (see VA Directive 5021).

(2) Providing appropriate information to PO for completion of PSETS entries in a timely manner regarding mitigation/disciplinary actions.

(3) Ensuring that appropriate disciplinary action is taken when privacy violations are brought to their attention.

(4) Coordinating with facility PO on the privacy and disclosure of personnel records and other records maintained by HRMS.

(5) Ensuring that personnel records maintained by HRM are maintained in compliance with applicable privacy policies, statutes, and regulations.

h. **VA Contracting Officer (CO)/Contracting Officer Representative (COR).** The CO/COR is responsible for:

(1) Determining the appropriate security and privacy language in all contracts by collaborating with the facility Privacy Officer to ensure that privacy responsibilities are included (see VA Handbook 6500.6, Appendix C). Ensuring through the COR that contractors are aware of, and abide by, those privacy responsibilities as stated in contracts with VA and VHA.

(2) Ensuring through the COR that contractors are aware of, and abide by, those privacy responsibilities as stated in contracts with VA and VHA.

(3) Ensuring that Business Associate Agreements are enacted for all in which the contractor meets the definition of a business associate. The Business Associate Agreements should be a separate document from the contract.

(4) Ensuring that the contractors receive the appropriate privacy and if applicable security training upon initiation of the contract and annually thereafter.

(5) Ensuring that contract performance meets privacy requirements including mediating and/or terminating the contract if information privacy requirements are not being met.

i. **Service Chiefs, Program Managers, Supervisors or designees.** An exampleof a designee would be an Automated Data Processing Application Coordinator (ADPAC). The personnel indicated above are responsible for:

(1) Identifying and protecting all III used by supervised personnel, including contractors and other workforce members.

(2) Ensuring that individuals are only provided access to III when authorized and the appropriate training has been completed such as in the case of volunteers. (Note: CWT, compensated work therapy, patients are prohibited to have access to PHI).

(3) Ensuring that III, whether computerized or printed, is secured when work areas under their supervision are unattended.

(4) Facilitate or provide training to new and existing personnel on roles and responsibilities for protecting III, to include the requirement that possible suspected privacy violations are reported to the Privacy Officer at the time of discovery.

(5) Identifying and assigning functional categories in accordance with the facility policy and ensuring that supervised personnel have only the minimum necessary access level required to carry out their authorized functions or assigned duties and that supervised personnel understand what their minimal level of access is and that access beyond the scope of their responsibilities will result in disciplinary action.

(6) Ensuring applicable personnel complete “Information Security and Privacy Awareness and Rules of Behavior” training. If access to protected health information (PHI), is required then “Privacy and HIPAA” training must be completed within 30 days of hire or before access to PHI is given. Training must be completed annually thereafter and documented using the Talent Management System (TMS). Workforce members must be enrolled in TMS either through self-enrollment (For example, contractors and volunteers) or automatic enrollment upon hire.

(7) Ensuring that media (paper, electronic, Compact Discs (CDs), disks, portable devices, etc.) with III is disposed of via approved means. Shredding is done by a contractor. They provide the containers as well as coordinate the shredding of the paper. Community Based Outpatient Clinics (CBOC) also use the same vendor for their shredding. Services will contact Environmental Management Services (EMS) when special arrangements need to be made regarding destruction of other media.

(8) Assisting the facility PO and Human Resource Management with the investigation and resolution of privacy incidents involving their employees and/or program(s). However, supervisors are not to access a record for investigation without express permission from the Privacy Officer.

(9) Provide all responsive documents to the FOIA Officer upon request in a timely manner and require cooperation from staff in response to all FOIA requests.

j. **Quality, Safety and Value Manager.** The Quality, Safety and Value Manager is responsible for coordinating with the facility PO, FOIA officer and ROI staff on requests for copies of or access to QM documents. The facility Privacy Officer serves as the final approval authority for determining which documents are classified as quality management documents in accordance with VHA Directive 2008-077, Quality Management (QM) and Patient Safety Activities That Can Generate Confidential Documents prior to disclosure. The facility Privacy Officer will work with the FOIA Officer concerning any exception to disclosure under FOIA.

k. **Administrator on Duty (AOD).** The AOD is responsible for resolving and responding to disclosure issues and incident reporting requirements consistent with VHA Directive 1605, VHA Handbooks 1605 series, VA Directive 6500 and VA Handbook 6500 series during non-business hours during the off tours.

l. **All individuals who have access to sensitive information.** All individuals who have access to sensitive information are responsible for:

(1) Accessing the minimum necessary data for which they have authorized privileges and, on a need, to-know basis in the performance of their official VA duties.

(2) Employees must exercise appropriate precautions and safeguards when discussing Veterans' individually identifiable information (III) in public areas to prevent an unauthorized disclosure.

(3) Protecting an individual's rights to privacy and ensuring proper use anddisclosure of information. All workforce members will be held accountable for compliance with these policies, procedures, and applicable laws.

(4) Appropriately safeguarding printed and electronic III.

(5) Reporting complaints and/or violations of privacy policies or procedures to the facility PO, or designee immediately upon discovery. Co-operating with the facility Privacy Officer and/or the VHA Privacy Office throughout the complaint investigation process.

(6) Cooperating with the facility Privacy Officer and/or the VHA Privacy Office throughout the complaint investigation process.

(7) Obtaining appropriate approval in accordance with Public Affairs policy to speak to the news media. Employees are not authorized to disclose any III on a patient or Veteran during an 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.

(8) Consulting the PO and VHA Directive Handbook 1605.01 for guidance in privacy situations not addressed in this document.

4. **PROCEDURES**

a. **Administrative Requirements.**

(1) The facility and its workforce will comply with the contents of this policy, VHA Directive 1605.01, and all other applicable privacy laws, regulations, and VA/VHA policies.

(a) The facility and its workforce will comply with the contents of this policy, VHA Directive 1605.01, and all other applicable privacy laws, regulations, and VA policies.

(b) The PO, or designee, will monitor compliance with this policy through various means, including continuous assessment for privacy compliance.

(2) **Documentation.** This policy and any changes thereto, must be maintained in writing, either on paper or in electronic form, for a period of at least six years. When VHA Directive 1605.01 is updated (which necessitates alteration of facility policies and procedures), the local privacy policies and procedures will be revised without delay. Medical Center Memorandums are reviewed yearly.

b. **Complaint Process.**

(1) All privacy complaints received by the facility are to be referred immediately tothe PO or designee for review and processing.

(2) An individual has 3 years from the date of the complaint to request an investigation into the alleged complaint. Health and Human Services, Office of Civil Rights (HHS-OCR) uses this same time frame for their complaints.

(3) The PO, or designee, will enter all facility privacy complaints, regardless of validity, into the VA Privacy and Security Event Tracking System (PSETS). AOD will report to PO any off duty after hour incidents. All incidents must be reported within one hour of discovery, during both normal business hours, as well as off duty hours to the VA Network Security Operations Center (CSOC).

(4) Notice to Privacy Complainants: All individuals filing a privacy complaint will be provided a copy of the Notice to Privacy Complainants at the time of the complaint submission.

(5) Complaints Identified as Incidents: When the facility PO makes a determination during the investigation that a privacy complaint is a privacy violation/incident, the PSETS ticket classification will promptly be changed from a complaint to an incident.

(a) If the complaint is made verbally, the PO, or designee will obtain mailing information to send the Notice to the privacy complainant.

(b) The Notice will be mailed to the privacy complainant within 10 working days if the Notice is not given in person to the complainant. A complaint acknowledgement cover letter will be included when the Notice is mailed.

(6) The facility PO, or designee, is responsible for investigating all complaints regarding facility privacy practices regardless of validity.

(a) Cooperating with the VHA Privacy Office on all HHS-OCR complaints and all other privacy complaints submitted to VHA Privacy Office in VHA Central Office (VHACO), in addition to providing timely access to complaint investigation files.

(b) Acknowledging receipt of privacy complaint by providing IB 10-69, Notice to Privacy Complainants in compliance with VHA Directive 1605.01.

(c) Communicating with leadership, as appropriate (i.e., Director, VISN, VHA Privacy Office, Office of InspectorGeneral, and Office of General Counsel).

(d) Determining whether a complaint is a privacy violation/incident and responding appropriately.

(e) Responding as soon as possible (or no later than 60 working days), in writing, to the complainant when the complaint does not result in an incident.

(f) Appropriately notating the privacy complaint/incident in PSETS.

(g) Documenting outcomes of the investigation and provide findings to the supervisor in coordination with other stakeholders (i.e., Human Resources for sanctions or disciplinary actions, union representatives, Service Chiefs, Program Managers).

(h) Mailing the response letter to the complainant’s address.

(i) Maintaining an administrative file for all complaints by PSETS ticket number or by date.

(j) Trending the types of privacy complaints identified and reports these trends to the facility leadership bi-annually and VHA Privacy Office, upon request.

(7) Complaints Identified as Incidents: When the facility PO makes a determination during the investigation that a privacy complaint is a privacy violation/incident, the PSETS ticket classification will promptly be changed from a complaint to an incident.

(a) When a privacy complaint is made regarding access to a health record and the facility PO cannot prove that the access is likely or not likely authorized, the access must be presumed to be unauthorized and will be reported as a privacy violation/incident in PSETS.

(b) All determinations as to whether a privacy incident warrants credit monitoring protection services or a notification only letter will be made by the VA Data Breach Resolution Service (DBRS) and the Data Breach Core Team (DBCT).

(c) The DBRS and DBCT will notify the facility PO in accordance with VA Handbook 6500.2, Appendix C.

(d) When required the notification letter or credit-monitoring letter will be mailed no later than 60 calendar days from when the incident was reported by the PO.

(8) Administrative Record Keeping: A privacy complaint file containing all the documentation of the privacy complaint and investigation will be retained by the facility PO in accordance with the Record Control Schedule (RCS) 10-1, item number 1006.19, Privacy Complaint File. Documentation in the complaint file will consist of the following:

(a) Initial written complainant's concern or a Report of Contact by the PO, if the complaint is made orally.

(b) Written documentation of all interviews or statements.

(c) All written correspondence, including emails.

(9) All complaints (privacy and/or security related) received from the Department of Health and Human Services (HHS)-Office for Civil Rights (OCR) will be encrypted and forwarded immediately to VHA Privacy Office mail group VHAPrivIssues@va.gov for appropriate processing. The facility does not have authority to respond to HHS-OCR complaints.

(a) If an investigation arises because of an HHS-OCR complaint, this facility and its business associates must permit the Secretary of HHS access to information, during normal business hours, after coordinating with the VHA Privacy Office.

(b) If the facility PO receives an HHS-OCR notification letter, this notification letter should be forwarded via encrypted email to the: VHAPrivacyIssues@va.gov Outlook mail group.

(c) When addressing complaints, the facility PO should reference resources available on the VHA Privacy Officer SharePoint site. When Human Resources is contemplating employee disciplinary action, they should refer to VA Directive5021 and VA Handbook 5021, Employee/Management Relations.

(10) The facility may not require an individual to waive any right under these provisions as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

(11) The facility may not retaliate against a person for exercising rights provided by the HIPAA Privacy Rule, for assisting in an investigation by HHS-OCR or another

appropriate authority, or for opposing an act or practice that the person believes in good faith violates these provisions.

c. **Reasonable Safeguards.**

(1) All facility workforce members shall ensure that appropriate administrative, technical, and physical safeguards are used to maintain the security and confidentiality of III, including protected health information (PHI), and to protect against any anticipated threats or hazards to their security or integrity. The facility's workforce shall make reasonable efforts to limit III to the minimum necessary to accomplish the intended purpose of any use, disclosure, or request. This does not pertain to the treatment provision under the HIPAA Privacy Rule.

(2) All personnel may access and use information contained in VHA records as required for their official duties related to treatment, payment, and healthcare operations purposes. Service Chiefs, or designees, will assure that employees have access to the information that is necessary to perform their duties. Supervisors will work with the PO/ISSO when necessary for any clarification.

(3) When disclosing VHA information, all applicable laws and regulations are reviewed and applied to the request to assure utilization of the most stringent provisions for all uses and/or disclosures of data in order to provide the greatest rights to the individual and the minimum necessary of III. III disclosure is mandatory with a valid written authorization, signed by the individual but disclosure must be limited to only the information necessary to satisfy the purpose of the request.

(4) Disposal of documents: Staff disposes of paper documents that contain III by ensuring all such documents are immediately placed in "locked" shredding collection receptacles located throughout VHSO facilities. Data that is not destroyed at the site of production, such as transported for contracted shredding, must be secured in locked containers or in locked areas until it is removed for destruction. CBOCs utilize the same shredding vendor. Facility follows processes as outlined in VA Directive 6371. Final destruction method meets the requirements of directive.

(5) Disposal of Electronic Media: Electronic media and electronic media storage devices such as CD and portable thumb drives containing III will be destroyed in accordance with Office of Information Technology (OI&T) Standard Operating Procedure.

(6) Non-paper items containing III (For example, wristbands, IV bag labels, labels/stickers) will be disposed of in the same manner as the paper process at VHSO. Labels/stickers will be removed form containers prior to placement in "locked" shredding collection receptacles.

(7) Maintaining auditory privacy: Staff only discusses patient care issues in appropriate areas, which allow the maintenance of auditory privacy. Facility staff does not discuss patient information in areas not conducive to confidentiality (For example, canteen, elevators, or hallways). Signs must be posted alerting Veterans to auditory

privacy concerns in the waiting areas. VHA health care providers and staff must refrain from discussing patient information within hearing range of anyone who is not on the patient's treatment team or does not have a need to know the specific patient information unless an emergent condition arises whereby auditory privacy cannot be maintained. Administrative staff should follow the same guidance in any discussion involving individually identifiable sensitive information (i.e. employee health or disciplinary actions). Appropriate safeguards include training all staff on auditory privacy to include:

(a) Using the Veterans Health Identification Card (VHIC) for identification upon check-in, if available.

(b) Using an appropriate tone of voice when speaking with the Veteran in a public area or during check-in.

(c) Only discussing the information necessary to accomplish the function (For example, not asking for the full SSN when the last four of the SSN is enough).

(d) Asking other Veterans in line for clinical check-in to wait a short distance away from the desk to allow a zone of audible privacy as opposed to being right behind the Veteran being assisted.

(e) Only calling Veterans back to an exam room, pharmacy window or other treatment area by name.

(f) Going behind closed doors to have discussions pertaining to the personal information of the Veteran.

(8) Use of facsimile (fax): When using fax technology, facility staff adheres to VA Handbook 6500. Information Security Program, VHA Handbook 1907.01, Health Information Management and Health Records; and VHA Directive 1605.01, Privacy and Release of Information.

(a) III is only transmitted via fax when necessary. Any disclosure of faxed information containing or requesting individually identifiable patient information must be accounted for in the ROI Plus software or on a manual spreadsheet.

(b) Any staff member utilizing facsimile as a means of transferring III must take the following steps to ensure that III is sent to the appropriate destination and not to a machine accessible to the general public:

(c) Verify the fax number prior to sending the fax and, to prevent misdialing, do not use pre-programmed numbers unless the number is tested prior to faxing. Periodically verify the fax numbers of frequent recipients. Ask those frequent recipients to notify the facility of any fax number changes.

(d) Use a fax cover sheet with an appropriate confidentiality statement, instructing the recipient of the transmission to notify the facility if received in error, must be sent

with all outgoing faxes. PHI should never be placed within the fax cover sheet as this negates the confidentiality statement on the fax coversheet.

(e) Notify the recipient before sending the fax in order to ensure that someone is present to receive the information or that the fax machine is in a secure location, suchas a locked room.

(f) Review the fax confirmation slip to verify that the confidential information went to the proper destination number. If there has been an error, immediately contact the incorrect recipient and request return or destruction of the fax.

(9) Email and information messaging applications and systems are used as outlined in VA policy VA Handbook 6500. These types of messages never should contain III, unless the authentication mechanisms have been secured appropriately (see VA Handbook 6500). Responding to a patient via email which contains protected health information should only be done through MyHealtheVet Secure Messaging.

(10) Mailing of Sensitive Information: Mailing of Veteran's correspondence such as copies of records, appointment letters may be done using the United States Postal Service (USPS). Envelopes, parcels, packaging, or boxes containing sensitive information must be secured in a manner that prevents unauthorized access, tampering, or accidental loss of contents. Window envelopes must show the recipients' names and addresses, but no other information. (See VHA Directive 6609).

d. **Mitigation.** To the extent practical, this facility mitigates any harmful effect known to have resulted from an improper use or disclosure of III. Mitigation may include but is not limited to operational and procedural corrective measures; re-training, reprimanding, or disciplining workforce members; addressing problems with any involved business associates; incorporating the chosen mitigation solution(s) into facility procedures. All known or suspected breaches of patient privacy must be immediately reported to the facility PO or designee.

e. **Sanctions.**

(1) All individuals who use or gain access to VA information systems or sensitive information must sign and adhere to the Rules of Behavior, which bind them to the legal and moral responsibility of preventing unauthorized disclosure. (See VA Handbook 6500, Information Security Program) This facility has established sanctions, which are applied against members of its workforce as appropriate, for failures to comply with privacy policies and procedures and Rules of Behavior.

(2) This facility has established a set of rules that describes the information privacy operations of the facility and clearly delineates the responsibilities and expected behaviors of all workforce members. These rules address all significant aspects of using III and the consequences of inconsistent behavior or non-compliance. The entire workforce of this facility will have access to a copy of these rules for purposes of review. A signed (manually or electronically) acknowledgement of these rules is necessary for each workforce member.

(3) The facility PO will determine information privacy violations and provide evidence thereof. The employee's supervisor will determine appropriate actions and may, in conjunction with human resources, take necessary steps and apply appropriate sanctions for any employees who are non-compliant with privacy policies and procedures. Penalties will be assessed against any individual(s) who knowingly and/or willfully use, disclose, or obtain information without the patients written authorization or not.

(4) Appropriate sanctions must be taken in accordance with VA Directive 5021.

(5) Adverse actions may include, but are not limited to, progressive discipline. The facility will follow processes and procedures outlined in VA Handbook 5021 for adverse actions in compliance with the stated Table of Penalties.

f. **Access to Sensitive Information and Restricted Areas.**

(1) All Individuals who have access to sensitive information are responsible for the following:

(a) Accessing the minimum necessary data for which they have authorized privileges and, on a need-to-know basis in the performance of their official VA duties.

(b) Protecting an individual's rights to privacy and ensuring proper use and disclosure of information. All workforce members will be held accountable for compliance with these policies, procedures, and applicable laws.

(c) Appropriately safeguarding printed and electronic individually identifiable information.

(d) Reporting complaints and/or violations of privacy policies or procedures to the facility Privacy Officer immediately upon discovery.

(e) Consulting the facility Privacy Officer and VHA Handbook 1605.1 for guidance in privacy situations not addressed in this document.

(f) All employees/visitors entering any area which has been designated as a restricted access area, will check-in at the door of the designated area, and inform staff of the reason for their visit.

(g) Following validation, the visitor will be asked to wait outside the designated area and wait to be escorted. Under no circumstances will any visitors be allowed to enter the restricted area without being escorted.

(h) All employees must pay particular attention to all access doors leading to restricted access areas and may only allow access when there is a valid business purpose.

(i) Employees must pay close attention when entering restricted areas, to ensure that no individuals are attempting to gain access by “tagging along” behind them.

(j) If an employee notices an individual that they do not recognize as being “authorized,” the employee should immediately “challenge” the individual and ascertain his/her reason for being in the area.

(k) If a valid reason cannot be determined, the employee should first ask the employee to wait outside of the restricted area, then contact facility management/supervision immediately and advise them of the situation.

(l) If the individual departs the area, a complete description of the individual should be provided to management/supervision and/or to VA Police/law enforcement if warranted.

(m) Employees must wear their PIV badge on the outside of their clothing, above the waist at all times unless it presents a safety hazard when performing their official duties.

g. **Privacy Training and Education.**

(1) The facility PO will conduct privacy training at all facility New Employee Orientation (NEO) programs.

(2) Employees are responsible for annual completion of their mandatory privacy training requirement prior to or on their anniversary date of privacy training the following year. Monthly, the PO reviews the delinquent HIPAA and Privacy training report generated by TMS. The PO emails the supervisor of the employee that is delinquent for follow through and completion.

(3) The facility Privacy Officer, in coordination with the facility Education Office, Service Chiefs, Program Managers, and supervisors, and their respective designees, assist in the process of compiling annual training records to report the facility privacy training completion status to the VHA Privacy Office and to the MCD upon request.

(a) The annual training records of completion of privacy training must be kept for all employees, volunteers, students, and contractors for reporting of facility privacy training completion numbers by each group.

(b) The MCD will certify annual training completion to the VHA Privacy Office for all work force members based on the reports generated by the Education Office upon request.

(4) The facility PO shall conduct other activities within the facility to enhance awareness of privacy and that have a positive impact on the overall privacy culture and posture of thefacility. These activities shall include, but are not limited to, participation in VA’s annual Privacy Week activities, posting privacy posters and announcements throughout the facility, and conducting one-on-one training with personnel who have been observeddisplaying negative privacy culture behaviors.

h. **Privacy Threshold Analysis**

(1) The Privacy Threshold Analysis (PTA) is an internal document used by the Privacy Officers, information system owners and the Information System Security Officers (ISSOs). Based on the information in the PTA, Privacy Impact Assessment (PIA) support determines if a PIA is required under the E-Government Act of 2002.

(2) PTAs identify programs and systems that are privacy-sensitive and contain PII. PTAs create an annual record of major system changes and standardize the privacy compliance process. PTAs strengthen the understanding of VA systems, programs, and projects. PTAs are written so that individuals who don't have a technical background can understand what's being stated.

(3) PTAs are to be completed and submitted to the VA Privacy Service PIA support mail group PIAsupport@va.gov on an annual basis unless there is a major change to an IT system prior to the annual review.

(4) PTAs are not publicly posted. To obtain a copy of an approved PTA, you may contact PIA Support at piasupport@va.gov.

i. **Privacy Impact Assessment**

(1) Privacy Impact Assessments (PIA) outline the risks and effects of collecting, maintaining, and disseminating PII. They mitigate potential privacy risks by evaluating protections, such as security and privacy controls. They can also introduce alternative processes for handling information.

(2) PIAs help identify the overall privacy risk level of a system, program, or project. PIA's inform leadership, program offices, and Veterans about how VA is implementing privacy and mitigating risks associated with PII collection, use, and maintenance.

(3) PIAs are to be completed and submitted to the VA Privacy Services PIA support mail group at PIAsupport@va.gov every three years unless there is a major change to the IT system prior to the three-year period.

(4) PIAs inform the public what PII VA is collecting, why the PII is being collected and how the PII will be collected, used, accessed, shared, safeguarded and stored.

j. **Personally Identifiable-Information Database Inventory**

(1) The facility Privacy Officer, in coordination with the facility Area Manager, ISSO, Records Manager and facility IT staff, shall maintain a process for identifying databases which collect or maintain PII/PHI.

(2) The PO ensures databases identified with PII/PHI are accounted for in existing PTA and PIA.

(3) If the databases identified are not accounted for, then the PO, in collaboration with the Area Manager and ISSO, updates the PTA and PIA documents accordingly.

(4) Database inventories are done on an annual basis.

k. **Individual Rights.**

(1) **Verification of Identity:**

(a) In order to receive or view information from his or her VHA record, an individual must present staff with adequate information for verification of identity, as outlined in VHA Directive 1605.01. Individuals may not verify identity by email.

(b) A VHIC, passport, driver's license, or employee identification card may be usedto identify an individual who appears in person. Mail or fax identification requests maybe verified by social security number, address, and signature comparison to the VHA record.

1. Legal Guardian: A person designated by a court of competent jurisdiction to manage the property and rights of another person who, due to defect of age, medical condition, understanding, or self-control, is considered by the court to be incapable of administering the individual's own affairs. Depending on the circumstances, the court may appoint a legal guardian for a specific purpose. A VA Federal fiduciary is not a legal guardian. Three of the most common types of guardianships are: Legal Guardian of the Person; Legal Guardian of the Property; and Legal Guardian of the Person and Property.

2. Power of Attorney (POA): All POAs are to be referred to the PO for determination that the POA meets the legal requirements for making disclosure decisions.

a. A personal representative of the deceased individual, who under applicable law has authority to act on behalf of the deceased individual. This may include power or attorney (if binding upon death), the executor of the estate, or someone under federal, state, local or tribal law with such authority. The next of kin of a deceased individual is considered a personal representative of the deceased individual but not of a living individual. They are recognized as having the same rights as the deceased individual. When there is more than one surviving next-of-kin, the personal representative will be determined based on hierarchy: spouse, adult child, parent, adult sibling, grandparent, or adult grandchild.

b. Regardless of the type or source of the POA presented, the reviewer always needs to carefully check the document with General and Special Powers of Attorney. The document must be in writing; signed by the individual giving the power; dated; notarized and signed by a licensed notary public; and specifically designate, by name, the third-party agent, which may be an organization or entity, to act on behalf of the individual.

(2) **Notice of Privacy Practices:**

(a) An individual will be provided with a copy of IB10-163, VHA Notice of Privacy Practices, by this facility upon verbal or written request. All Veterans receive a copy of this notice from the Health Eligibility Center upon enrollment.

(b) An individual may obtain a copy of IB10-163, VHA Notice of Privacy Practices, from Eligibility, Emergency Department, and/or ROI.

(c) All Non-Veteran who receives care and treatment at VHSO whether for humanitarian purposes or a VA research study must be given a copy of the VHA Notice of Privacy Practices at the time of check in. VA Research staff would provide the non-Veteran with copy of the notice and get the form signed when consenting them. The completed acknowledgement forms, VA Form 10-0483 are to be sent to the PO and will be scanned into the medical record.

1. In an Employee Health situation, an Employee Health staff member may maintain a copy of the acknowledgement form in a binder or in the blue employee health folder if applicable. CPRS should be used only if there is not another place to keep the acknowledgement form.

2. The facility Privacy Officer utilizes audit form and goes to Employee Health to review documents. PO audits those that are done by Eligibility staff utilizing information received from them. Research notifies PO as well as PO makes a note when non-Veteran protocols are reviewed. VHA Handbook 1605.04 provides guidance.

(3) **Right of Access:**

(a) If access is legally appropriate, individuals may obtain a copy of, or inspect, their record or III. A request to obtain a copy or inspect their record must be made in writing by the individual or a personal representative. Individuals may use VA Form 10-5345a, Individuals Request for a Copy of their Own Health Information, to accomplish this purpose.

(b) All requests for copies of individuals' own health information will be made in writing and directed to the Release of Information Department. All requests must show date received whether by use of a date stamp, writing date received on request, or entering the request in ROI Plus software the exact same day as received in person or mail.

(c) 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 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.

(d) If the individual or the individual's representative is not entitled to the records under any legal provisions, this facility will not provide them with a copy of the records.

NOTE: *This is an infrequent occurrence. The facility Privacy Officer should be consulted prior to such a denial.*

(e) Access to view a record must be processed as follows:

1. 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 (For example, reproducing magnetic tape records in a hard copy form readable by the individual), necessary arrangements must be made for a later personal review or, if acceptable to the individual, copies may be furnished by mail.

2. Mailed requests must be referred to the facility Privacy Officer for determination if the right of access review will be granted.

3. If additional information is required before a request can be processed, the individual requesting review must be advised what information must be provided to complete the request.

4. 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 providedby mail, if the individual has indicated that a copy is acceptable.

(f) All right of access requests, granted requests, and denials are documented in the ROI Plus software, in accordance with VHA Directive 1615, Mandated Utilization of ROI Manager Software. Other Services where individuals are provided copies of their own information and which do not use the ROI Plus software (i.e., Human Resources, Research, Police and Security, Credentialing and Privileging, Employee Health, Infection Control, Fee Basis, Consolidated Patient Accounts Center, Quality Management, etc.) will submit data about these releases to the PO or to ROI for tracking of disclosures and inclusion in the annual FOIA report.

(4) **Amendment Request:**

(a) An individual has the right to request an amendment to any information or records retrieved by the individual's name or other unique identifier contained in a VA Privacy Act system of records, as outlined in VHA Directive 1605.01. A request for name change is considered an amendment request and must have the appropriate legal documents for the Master Person Index (MPI) Coordinator to make the change.

(b) 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 lockedfile cabinet or scanned to a secure network drive but cannot be scanned into the administrative portion of VISTA Imaging in the health record.

(c) The amendment file must be retained and destroyed in accordance with RCS 10-1, Privacy Amendment Case File. under Section 1006.9. 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.

(d) Amendment requests are delivered to the facility Privacy Officer. The request must be mailed to Release of Information, 1100 North College Avenue, Fayetteville, AR 72703 or hand delivered to Release of Information at the main campus. These requests are then delivered to the Privacy Officer.

(e) Requests to amend records are acknowledged by the facility Privacy Officer in writing within 10 working days of receipt. The review process must be completed as soon as possible, in most cases, within 30 working days from receipt of the request, but not more than 90 calendar days from the receipt of the request. The facility PO or designee will send subsequent notices when necessary.

(f) The facility PO will refer the request to the health care provider who authored the information for the provider to determine if the record needs to be amended as requested.

(g) When an amendment is approved, the following actions are taken:

1. Information that is requested for deletion must be made illegible, e.g. marked through, in the paper record. For electronic records, the Chief, HIMS is required to use the Computerized Patient Record System (CPRS) Text Integrated Utility (TIU) functions for amending documents. For all other records, the Chief, HIMS will work with the responsible record custodian to amend theirrecords (For example, police or employee records).

2. Any new material must be recorded on the original document. For paper records, the words "Amended-Privacy Act and/or 45 CFR Part 164" must be recorded on the original document. New amended material may be recorded as an addendum if there is no room on the original document; however, the original document should state that there is an addendum. 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. The amendment must be validated with the date as well as the signature and title of the person making the amendment. For electronic records, Veterans Health Information Systems and Technology Architecture (VISTA) will automatically place the appropriate notation on amended records.

3. For an electronic amendment of a TIU (Text Integration Utility) document, the Chief of 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.

4. The individual making the request must be given a copy of the amended record and be advised in writing that the record was amended. The individual must also identifyand agree to have notification sent to any relevant persons or organization who they gave copies of their record to. 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.

5. 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.

(h) When a request to amend a record is denied, the Chief, HIMS or designee, or the facility PO, or designee, must promptly notify the individual making the request. The written notification will contain all the required elements outlined in VHA Directive 1605.01 and:

1. Instruction that the individual may also provide a statement of disagreement to the facility and request that the facility provide the statement of disagreement with all future disclosures of the disputed information. A statement of disagreement is to be no longer then two pages in length, an individual may submit a longer statement if it is necessary to set forth the disagreement effectively, however the PO or Chief of HIMS will make the determination to accept it or not.

2. The name or title and telephone number of the person or office of contact.

3. The signature of the MCD.

4. Advisement of appeal rights (the individual may appeal to the Office of General Counsel (024), 810 Vermont Avenue N.W. Washington, DC 20420). If the 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 VA healthcare facility that made the initial decision.

(i) Should the individual choose to have their amendment request and the agency's subsequent denial attached to future disclosures, the Chief, HIMS identifies the III thatis the subject of the disputed amendment and appends, or otherwise links, the individual's request for an amendment, and the facility's denial of the request, to the individual's record.

(5) **Confidential Communications Request:**

(a) An individual's oral or written request to receive any or all types of communications (correspondence) from facility staff via a confidential alternativemeans, or at an alternative location, must be processed in accordance with Members Service Knowledge Management Web site.

(b) All confidential communications requests will be referred to Eligibility, the emergency department, or Privacy Officer.

(c) When the Veteran makes the request of a staff member to allow for the receipt of written communications at an alternative address other than the permanent address of record:

1. Veterans must specify a start date for use of the confidential correspondence address. Dates occurring in the past are not acceptable. Patients may specify an end date for use of the address, but it is not required.

2. The staff member must access the proper VISTA menu option and answer the prompts. VISTA allows the capture of the new confidential communications address fields including date started and stopped; the street address; city; state; and zip code including the four digits geocode, and country.

(d) Requests to split communications under a correspondence type are considered unreasonable and will be denied. With an exception to My HealtheVet, a request to receive communications via electronic mail is also to be considered unreasonable and will be denied.

(e) A confidential communications address that results in undeliverable mail is considered invalid; and that the correspondence is resent or re-mailed to the individual's permanent address as notated in VISTA.

(f) When a confidential communications address is activated for medical records, the address is viewable through the ROI Plus software for utilization by the ROI Clerks.ROI Clerks must use the confidential communications address when activated to provide individuals with copies of their own records regardless of the address on the request without further communication with the individual and subsequent change withinVISTA.

(6) **Restriction Request:**

(a) An individual's requests for restrictions on the use or disclosure of their IIHI thatis used to carry out treatment, payment, or health care operations are referred to the PO. All restriction requests must be made in writing. ***NOTE:*** *A verbal request by the Veteran to not share their information is not a restriction request. A facility health care provider may NOT grant a restriction request. The provider must refer the individual toROI for consideration. ROI staff will coordinate with the facility PO regarding the request.*

(b) All requests for restrictions of IIHI need to be reviewed on a case-by-case basis by the facility PO or designee. If the facility is considering granting the request, the VHA Privacy Office should be consulted. Restrictions are not considered unless they meet the following criteria:

1. Submitted in writing.

2. Identify which information is to be restricted.

3. Identify who the information is to be restricted from.

4. Indicate for what purposes (For example, use for payment) the identified information is to be restricted.

5. Signed and dated by the individual to whom the record pertains.

(c) Although VHSO is not required to agree to restrictions requested by individuals, any restriction granted must be appropriately documented. If a request for restriction is granted, all facility programs and employees must adhere to the restriction unless the information covered by the restriction is needed to provide a patient with emergency treatment. The records will be appropriately flagged to alert all staff with access to the restriction.

(d) When a restriction request is denied, the PO or designee promptly informs the individual of the decision. The notification includes the reason for the denial and the signature of the MCD or designee. All restriction requests and denials are documented and retained in the ROI Unit. There are no appeal rights given for a denial of a restriction request.

(e) When deemed appropriate a prior granted restriction request will be terminated. The facility Privacy Officer will inform the individual in writing of the facility termination of the restriction and that such termination is only effective with respect to protected health information created or received after the notification date.

(7) **Facility Directory Opt-Out:**

(a) Individuals may request exclusion from the Facility Directory during each inpatient admission, in accordance with the Chief Business Office Procedure Guide 1601B.02. The facility Directory Opt-Out provision does not apply to Emergency Rooms unless the patient is going to be admitted to an inpatient setting. The facility Directory Opt-Out provision does not apply to Outpatient clinics. ***NOTE:*** *The procedure guide can be found at:* *http://vaww.va.gov/CBO/apps/policyguides/infomap.asp?address=VHA_PG_1601B.02.2.E.4.* *This is an internal VA website that is not available to the public*

(b) Upon admission, VISTA will prompt the user to select either opt-in or opt-out for each inpatient in the facility directory. During the admission screening process, the Admissions staff will ask each inpatient to specify whether he or she wishes to be excluded from the facility directory and document their decision in the VISTA system at each admission episode.

(c) VISTA should be edited utilizing either the Admit a Patient or Extended Bed Control options to indicate the patient's preference.

(d) Each patient must be advised that if they request to be excluded, medical center staff will not be permitted to provide any information to visitors or callers concerning

whether a patient is an inpatient at the facility. This includes family, friends, colleagues, deliveries (i.e., flowers, cards, etc.) or anyone asking about the patient.

(e) A patient may, at any time during an admission, change the initial decision to be included or not in the facility directory.

(f) If an inquiry is received concerning a patient who elects to opt-out of the facility directory, the sample response may be “I am sorry, but I do not have any information I can give you on whether John Q. Veteran is a patient.” All inquiries regarding patients who have opted out of the facility directory should be forwarded to the ROI during the normal duty day, and to the AODs afterhours.

(g) If the patient is incapacitated or unable to make this decision at the time of admission, the facility healthcare provider admitting the patient decides based on the patient’s prior admissions and the best interest of the patient.

1. The provider must document this decision in the patient’s medical record in CPRS.

2. Once the patient can communicate or make the facility directory opt-out decision, the patient must be given an opportunity to do so. Staff on the unit will discuss with the patient and contact Eligibility to make the change in the record.

3. The PO works with the admission staff as well as providers educating them to this requirement with the assistance of the Chief of Staff.

(8) **Accounting of Disclosures:**

(a) The facility maintains an accounting of all disclosures of III for six years after the date of disclosure or for the life of the record, whichever is longer. (See RCS 10-1 for additional guidance or the Records Manager.) This accounting includes disclosures made with or without patient authorization, although disclosures of data to VHA employees performing their official duties regarding treatment, payment and health care operations, under a traditional FOIA request, to the individual under Right of Access and disclosures of de-identified data do not require an accounting.

(b) In most circumstances, the accounting will be maintained electronically via the most current version of the ROI Plus software as part of the record from which the disclosure was made. See VHA Directive 1615, Mandated Utilization of the Release of Information (ROI) Plus software.

(c) The Accounting of Disclosures in areas that do not utilize the ROI Plus software (i.e., Office of Community Care, Infection Control, Police, Credentialing and Privileging, Employee Health, QM and Human Resources) will utilize the spreadsheet developed for tracking the processing of any requests received. If assistance is needed, the Service will contact the PO and/or Chief, HIMS. The spreadsheets from the various areas are submitted to the PO quarterly.

(d) An individual may request a copy of an accounting of disclosures from their records. The request must be made in writing, signed, and adequately identify the system of records or designated record set(s) for which the accounting is requested.The request must be delivered to the PO so that a date can be put on the request for processing and completion within the 60 calendar days.

(e) Accountings must contain the name of the individual to whom the information pertains, date of each disclosure; the nature or description of the disclosed information; a brief statement of the purpose of each disclosure, or in lieu of such statement, a copy of a written request for each disclosure; and the name and, if known, address of the person or agency to whom the disclosure was made.

(f) The accounting of disclosure must be made available within 60 calendar days of the facility's receipt of the request, except for disclosures made for health oversight activities or law enforcement purposes authorized by 38 CFR 1.576(b)(7) and 45 CFR 164.528(a)(2)(i).

1. If the accounting cannot be provided within the specified timeframe, the timeframe may be extended 30 days.

2. In order to extend the timeframe, the requestor must be issued a written statement from the PO that includes the reasons for the delay and the date by which the accounting will be provided. Only one such extension of time for action on a request for an accounting of disclosures is permitted.

l. **Uses and Disclosures:**

(1) **Minimum Necessary:**

(a) The minimum necessary requirements do not apply to disclosures to, or requests by, a healthcare provider who requires the information for treatment purposes.

(b) All facility staff should have minimum necessary (for completion of job duties) access to PHI. Specific minimum necessary policies and procedures, including appropriate staff access levels, are explained in VHA Handbook 1605.02, Minimum Necessary Standard for PHI. Functional categories are assigned per policy by the supervisor.

(c) Utilizing the guidance from VHA Directive 1605.02, the Service will work with the PO to assure that only the minimum necessary information is provided to staff.

(2) **Authorizations:**

(a) VHSO does not use or disclose III without appropriate authority conferred by applicable federal privacy laws and regulations or individual written authorization. Valid authorizations are used only for the purpose(s) stated in the authorization and only disclosed by or released to the personnel or office listed in the authorization.

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

1. VHSO needs to utilize III for a purpose other than treatment, payment, and/or healthcare operations, and other legal authority does not exist, and

2. VHSO discloses information for any purpose for which other legal authority does not exist.

(c) An authorization to release information must be made in writing and include the following information:

1. The identity (i.e., name, date of birth and last four of the social security number)of the individual to whom the information pertains.

2. Veteran Request: If 38 U.S.C. §7332 protected health information is to be disclosed, this information must be specifically identified by checking the boxes.

3. If the authorization indicates specific 38 U.S.C. § 7332 protected health information is to be released to include future health information with a future expiration date, but the Veteran does not have the indicated 38 U.S.C § 7332 protected diagnosis at the time of signature, the authorization is considered to be invalid for any future 38 U.S.C. § 7332 protected information acquired after the signature. This newly acquired 38 U.S.C. § 7332 protected information cannot be disclosed without a new authorization being obtained. Marking all boxes on VA Form 10-5345 for 38 U.S.C § 7332 protected information is not acceptable practice. If the Veteran marks all 38 U.S.C § 7332 boxes and does not have the diagnoses and this authorization is for a one-time use, then the authorization is still valid.

4. A description, which identifies the information in a specific and meaningful fashion, of the information to be used or disclosed.

5. The name of the person(s) or office(s) authorized to make the requested use ordisclosure.

6. The name or other specific identification of the person(s) or office(s) to which the agency may make the requested use or disclosure.

7. A description of the purpose(s) for the requested use or disclosure. A statement“insurance purposes” etc. is enough. A purpose is not required when disclosing the information to the individual to whom the information pertains.

8. An expiration date, condition or event that relates to the individual or the purpose of the use or disclosure of the information. If the purposes section is not filled out and there is no expiration date, condition or event, the authorization is considered invalid. Examples of appropriate expiration date language specific to research are:

9. Authorization may be given:

a. On VA Form 10-5345, Request for and Authorization to Release Medical Records or Health Information, or any subsequent authorization form approved to replace this form, or a specific authorization developed for a specific VA program, (For example, eHealth Exchange Mission Act).

b. Using an outside entity's authorization form (For example, Social Security Administration Authorization form) if all the authorization content requirements are met.

10. Information will not be disclosed based on an authorization form that:

a. Fails to meet all the preceding requirements.

b. Has expired.

c. Is known to have been revoked.

d. Has been combined with another document to create an inappropriate compound authorization.

e. That is known, or in the exercise of reasonable care should be known, to facilitystaff as false with respect to any item of the authorization requirements.

(d) The ROI Unit will provide further guidance regarding authorizations that are not valid and the necessary corrective actions.

(e) If an authorization form is determined to be invalid, the ROI Unit will notify the requestor of the deficiencies.

(3) **Authorizations for documents protected by 38 U.S.C § 7332:**

(a) Information on testing for HIV and sickle Cell Anemia is no longer considered protected; therefore, this information may be disclosed without an authorization.

(b) If 38 U.S.C § 7332-protected health is to be disclosed for any purpose other than treatment, this information must be specifically identified in the authorization either by checking the boxes on VA Form 10-5345, Request for and Authorization to Release Medical Records or Health Information or by descriptive language on an outside entity's authorization form.

(c) Facility staff will not check off any of the 38 U.S.C. § 7332 boxes on the VA Form 10-5345, Request for and Authorization to Release Medical Records or Health Information unless the individual is specifically asked in person while a clerk completes the form for the individual prior to signing or a telephone discussion with the individual before mailing the authorization for signature. Staff may not arbitrarily check off boxes without the individual's oral approval. Oral approval is documented in the comments section of the ROI software.

(d) If the authorization indicates specific 38 U.S.C. §7332-protected health information is to be released to include future health information with a future expiration date, but the Veteran does not indicate 38 U.S.C. §7332-protected diagnosis at the time of signature, the authorization is considered to be invalid for any future 38 U.S.C. §7332-protected information acquired after the signature. This newly acquired 7332-protected information cannot be disclosed without a new authorization being obtained. If the Veteran marks all 38 U.S.C. §7332 boxes and does not have the diagnoses AND this authorization is for a one-time use, then the authorization is still valid.

(4) **Release of 38 U.S.C. §7332 for the purpose of treatment with Authorization:**

(a) The patient may check the box on VAF 10-5345 indicating he does not want 7332-protected information released for the purpose of treatment per that specific authorization form. However, the request for restriction on disclosure will not be honored for subsequent authorizations or any disclosure made for treatment without an authorization. Per the VA Mission Act, Public Law 115-182 on June 6, 2018, 38 U.S.C. §7332 was amended to permit disclosures to non-VA entities for purpose of providing health care to patients relating to HIV, sickle cell anemia and substance abuse without a signed, written authorization from the patient.

(5) **Producing and Using Video, photographs, audio or voice recordings:**

(a) In accordance with VHA Directive 1078(1), 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 must be used when VHA is producing or using images unless consent is not required per policy.

(b) In accordance with VHA Directive 1078(1), VA Form 10-3203a Informed Consent and Authorization for Third Parties to Produce or Record Statements, Photographs, Digital Images or Video or Audio recordings by VA must be used when VHA is agreeing to a third party interviewing an individual.

(c) VHA must also obtain an authorization from the patient or personal representative using VA Form 10-5345, **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. Refer to VHA Directive 1078(1), Privacy of Persons Regarding Photographs Digital Images and Video or Audio Recordings, for additional guidance.

(6) **Processing a Request for Release of Information:**

(a) Anyone may request VHA to disclose any record. Any request for information maintained in VHA and facility records must be processed under all applicable confidentiality statutes and regulations as well as in accordance with VHA Directive 1605.01.

(b) A request for copies of facility records must be in writing and describe the record(s) sought, so it may be in a reasonable amount of time.

(c) All written requests for copies of individually identifiable information maintained within the facility will be forwarded to the ROI Unit except as indicated below. The facility PO will be consulted on any requests received that are unusual or are not addressed in VHA Directive 1605.01 or this Medical Center Policy.

(d) CPAC Facility Records Manager or equivalent, is responsible for disclosing billing information. Revenue staff is also responsible for coordinating with ROI staff in order to account for disclosures of health information.

(e) Areas that do release information (i.e. Radiology) coordinate with ROI.

(f) The ROI staff will need to determine who is making the request for a copy of the facility record or information.

1. If the requestor is the individual to whom the records pertain, follow the guidance above in section 2.0. Right of Access.

2. If the requestor is other than the individual to whom the record pertains (third party), determine what information or record is requested and for what purpose and is there a written valid authorization from the individual or other legal authority prior to disclosure.

(g) The ROI staff will determine what information is being requested.

1. If the information requested does not contain individually identifiable information, provide the request to facility FOIA Officer for processing in line with VHA Directive 1935.

2. If the information requested contains individually identifiable information, review VHA Directive 1605.01 paragraph 16 and subsequent paragraphs for applicable guidance.

3. If the request is on a deceased individual, process the request in accordance with VHA Directive 1605.01 paragraph 34.

(h) The ROI Department must process requests for individually identifiable information within specified time standards and charge the applicable fees, as outlined in VHA Directive 1605.01.

1. Requests for copies of III must be answered within 20 workdays from the date of receipt.

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

3. Copying fees may be charged for copies of records provided to requestors. Onlycopying fees as stated in 38 CFR §1.577(f) or subsequent regulations may be charged. VHSO is prohibited for charging more for copies than is allowed in VA regulations.

(i) A requestor may request that the facility disclose or provide individually identifiable information in an electronic format, such as on CD, in lieu of paper copies. When the records requested exist electronically and can be reproduced in the request format, the facility must accommodate such a request. The ROI staff will process requests when records are requested in an electronic format.

(7) **Uses/Disclosures for Treatment, Payment, and Health Care Operations, and Other Operations Not Requiring Authorization:**

(a) VHSO uses and discloses IIHI as permitted by the HIPAA Privacy Rule, the Privacy Act of 1974 and other federal rules and regulations as permitted in VHA Directive 1605.01.

(b) Individuals are not required to and cannot be forced to waive their rights under the HIPAA Privacy Rule, 45 CFR § 160.306 as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

(c) The VHSO workforce (staff, employees, volunteers) uses and discloses IIHI inthe following manners:

1. Within VHA on a need-to-know basis for treatment, payment, and/or health careoperations without the written authorization of the individual.

2. To the extent necessary, on a need-to-know basis, and in accordance with goodmedical and/or ethical practices, staff may disclose general patient information to the patient's next-of-kin. If the patient is listed in the facility directory, staff also may discloseto the general public, without authorization, the patient's location and general condition.

3. To next-of-kin and family members in the presence of the individual if the patientdoes not object or if it is reasonably inferred from the circumstances that the patient does not object.

4. To next-of-kin and family members when, in the professional judgment of attending medical center staff members, disclosure is in the best interest of the patient.

5. To Veterans Benefit Administration (VBA) for use in the determination of eligibility for, or entitlement to, benefits.

6. To VA contractors or business associates for a contracted service or service provided on behalf of the facility related to treatment, payment, and/or health care operations provided that the disclosure is within the scope of the contract or agreement and a signed BAA with the contracted company or business associate is on file.

7. To a receiving facility when a patient is transferred to or being treated at a community hospital (including other federal hospitals), State Veteran Home, or community nursing homes.

8. To the Office of Resolution Management (ORM) when necessary for determining compliance with Equal Employment Opportunity (EEO) requirements and upon the request of the Office of Resolution Management.

9. To the Board of Veterans Appeals for benefits, including the processing and adjudication of claims appeals.

10. To the National Cemetery Administration for determinations of eligibility for, orentitlement to, benefits.

11. To VA Unions, while fulfilling their representational responsibilities. VA Unionsmay make a request to management for copies of facility records pursuant to its authority under Title 5 USC § 7114(b) (4). Unions may request any records that are maintained by a VA facility. This might include releasable portions of completed Administrative Investigation Boards (AIB), patient medical records and/or an employee's personnel records. However, under certain circumstances, unions may not be legally entitled to receive IIHI, or information protected by other statutes such as the Privacy Act. All requests for information submitted by VA Union Representatives are referred to the servicing HRMS, which coordinates the response with the Regional Counsel and the PO and/or the facility FOIA Officer (or designee).

12. To a Member of Congress (including a staff member acting on the Member's behalf) when responding to an inquiry from a Congressional office that is made at the request of the individual to whom the information pertains under the following conditions:

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.

c. If the constituent's inquiry is from the personal representative of the individual towhom 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.

d. Congressional requests are routed through the Director's Office. Upon receipt ofan inquiry, staff contacts appropriate Service(s) to complete the request in a timely manner. The Director's Office sends out the response once the information has been collected and processed.

13. 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.

14. To General Counsel and/or Regional Counsel for the purposes of health care operations (legal services) if a BAA is in effect. In addition, information may be provided to the Office of General Counsel (OGC) for any official purpose authorized by law if VHA Central Office maintains a Memorandum of Understanding or BAA with OGC authorizing the sharing of IIHI for legal counsel provided to VHA.

15. Except for criminal law enforcement activities, to the VA Inspector General or Office of Inspector General (OIG) Investigators for any official purpose authorized by law, such as healthcare oversight.

16. A Whistleblower 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.

17. 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 healthcare 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.

18. Except for criminal law enforcement activities, to the facility VA Police for enforcement of physical security (For example, escort of high-risk patients).

19. Veterans Health Information Exchange (VHIE) - The health information shared is a pre-determined standards-based set of clinical data that is sent to the requester through the Exchange. Direct access to the Veteran's health record is not involved and only requested information is exchanged via a virtual architecture with the non-VA health care provider who has an established treatment relationship with the Veteran. Veterans are automatically opted-in for the Exchange but may opt-out of sharing by filing VA Form 10-10164 online or at their closest VA Medical Centers' Release of Information Office (ROI).

20. To the VA Office of Employment Discrimination, Complaints, and Adjudication(OEDCA) to review the merits of employment discrimination claims filed by present andformer VA employees and non-agency applicants for employment.

21. The VHA Office of Medical Inspector (OMI) addresses health care problems tomonitor 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 toprovide a written request.

22. To the United States Office of Special Counsel (OSC). 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. VHA may disclose individually identifiable information to investigators who have been tasked to investigate the Whistleblower complaint. 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.

23. VA Human Resources Management Services (HRM). VHA may disclose individually identifiable information to VA HRM as authorized by law. 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.

24. Requests from Courts and Quasi-Judicial Bodies: Disclosure must be in accordance with VHA Directive 1605.01 and requests from Courts and Quasi-Judicial Bodies should be referred to the facility Privacy Officer who will consult with legal counsel as necessary. Subpoenas are not acceptable authority for the disclosure of III.

25. 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 not be protected under the Whistleblower Protection Act and may result in disciplinary action.

26. VA Researchers:

a. 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, other applicable 1200 handbook series, and 38 CFR Part 16.

b. For use or disclosure of individually identifiable health information involving non-employee research subjects for research purposes follow process outlined in VHA Directive 1605.01 paragraph 13.

c. If the research involves pictures or voice recordings for other than treatment purposes, the Informed Consent (10-0086) must state that a photograph, image or video/audio recording is going to be made. If the documentation of the Informed Consent form is waived, the script for the audio-recording must include the subject's permission to be recorded.

(d) Use of a patient's photograph or voice for purposes other than the identification, diagnosis, or treatment of the patient is not permitted unless a signed consent is obtained on 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 (38 CFR § 1.218). If photographs are taken to support treatment, those photographs are included in the medical record maintained for each patient and do not require VAF 10-3203. Disclosure of the patient's photograph or voice would require written authorization on VAF 10-5345 from the individual or personal representative. (See VHA Directive 1078(1), Privacy of Persons Regarding Photography, Digital Images and Video or Audio Recording).

(8) **Deceased Individuals:**

(a) Except for uses and disclosures for research purposes discussed in Section C. Uses and Disclosures, 10.0 Research Activities; VHSO shall protect the PHI of a deceased individual in the same manner, and to the same extent, as required for thePHI of living individuals.

(b) PHI, excluding 38 U.S.C. § 7332 information, of a deceased individual may be disclosed to coroners, medical examiners, and funeral directors. Title 38 U.S.C. § 7332 protected health information maybe be disclosed for determining cause of death or vital statistics per State law.

(c) PHI of a deceased individual may be disclosed for other reasons when legal authority exists.

(d) Disclosure of autopsy findings:

1. A copy of the autopsy clinical finding summary and the listing of clinical-pathological diagnoses on Standard Form (SF) 503, Medical Record-Autopsy Protocol, are disclosed, when requested by the next-of-kin.

2. All cases in which the autopsy reveals drug abuse, alcoholism or alcohol abuse,HIV infection, or sickle cell anemia information (which is subject to additional disclosure restrictions), the autopsy results are not disclosed to the next-of-kin unless the PO has determined that such disclosure is necessary for the survivor to receive benefits.

(9) **Contracts and BAAs:**

(a) In contracts/agreements that involve the use or disclosure of PHI, appropriate privacy requirements, specifications, and statements of work must state that privacy

requirements and specifications should be properly implemented before the contract/agreement goes into operation.

(b) All contracts must meet the contracting requirements dictated by VA's Office of Acquisition and Materiel Management and the Federal Acquisitions Regulations (FAR). Any contract which necessitates the use of III must conform to the policies and procedures in FAR Subpart 24.1, Protection of Individual Privacy and VA Handbook 6500.6, Contract Security.

(c) The Contracting Officer, the Privacy Officer, and the ISSO will work together to identify those entities that qualify as Business Associates under HIPAA and ensure that BAAs are enacted for these identified entities in accordance with HIPAA and BAA policies and procedures. ***NOTE:*** *A business associate relationship exists if the facility is required to release PHI to a contractor or business partner for the provision of services on the facility's behalf.*

(d) All contracts, agreements, and relationships must be assessed to determine if a business associate relationship exists. (See website) http://vaww.vhadataportal.med.va.gov/PolicyAdmin/BusinessAssociateAgreements.aspx.

(e) If a business associate relationship is determined to exist, a BAA is enacted utilizing only the most current version of the VHA Health Information Access Office-approved BAA language available at http://vaww.vhadataportal.med.va.gov/PolicyAdmin/BusinessAssociateAgreements.aspx.

(f) If a business associate is determined to serve more than one VA facility, the facility PO contacts the VHA Health Information Access Office to discuss enacting a national BAA. BAAs are kept updated and documented if the agreement is in force. Any national BAA takes precedence over a local BAA. Local and regional BAAs should not be initiated if a national BAA exists for the same services as described in the national BAA preamble. BAAs are kept updated and documented if the agreement is in force. (Refer to VHA Handbook 1605.05, BAAs.)

(g) Per the agreement, business associates will abide by the terms and conditions spelled out in the agreement.

(h) If a pattern of activity or practice of the business associate constitutes a material breach or violation of the business associate's obligation under the contract or other agreement is discovered, the PO reports the problem to the NSOC and works with the Contracting Officer to find a solution to the problem. All Business Associates must report the breach within 24 hours to the Director of Health Information Governance and submit a written report within 10 days.

(i) The Contracting Officer's Technical Representative (COR) responsible for the contract will monitor compliance with the applicable privacy policies required under the BAA with assistance and in consultation with the PO.

(10) **Emergency Situations and Serious/Imminent Threats:**

(a) When an employee becomes aware of a threat to the patient, another individual (For example, family of Veteran) or to the public, VHSO staff should contact the facility PO in order to determine if, and how, to report or address the serious and imminent threat to the health or safety of the patient, other individual or public.

(b) Facility initiated disclosures to a person or person(s) reasonably able to prevent or lessen a serious and imminent threat to the health or safety of the public requires approval of the facility Privacy Officer or is in accordance with the below paragraphs. Such persons may include, but is not limited to law enforcement, other health care providers, including nursing homes, or the individual threatened when there is no other legal authority to make the disclosures.

(c) When a local law enforcement agency approaches VHSO staff to obtain health information on a Veteran or patient due to a current or ongoing serious and imminent threat to the public, the facility PO and VA Police should be contacted.

1. During regular business hours, the facility PO will make the disclosure of requested health informationto the law enforcement officials in a position to prevent or lessen the threat. Such disclosure should be made immediately once the facility is made aware of the serious and imminent threat. If health information is needed after hours, the AOD should be contacted by VA Police to assist local law enforcement officials in obtaining informationto lessen or prevent the threat.

2. If health information is needed after hours, the AOD should be contacted by VA Police to assist local law enforcement officials in obtaining information to lessen or prevent the threat.

3. VA Police VA Police should never release IIHI to local law enforcement without consulting the facility Privacy Officer. VA Police Records, including Uniform Offense Reports, in the Police IT System are not IIHI.

(d) Disclosures may be made to the Centers for Disease Control (CDC) or State Public Health Agencies when there is a serious and imminent threat to the public and society, such as with COVID-19 pandemic, when other public health legal authority for the disclosure is not present.

1. 5 U.S.C. § 552a(b)(8)- to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if, upon such disclosure, notification is transmitted to the last known address of the individual to whom the records pertain, and

2. 45 CFR § 164.512(j)(1)(i): to avert a serious and imminent threat to the safety ofan individual as long as the disclosure is made to a party which is in a position to prevent or lessen the threat, such as a law enforcement official or the individual threatened, or

3. 45 CFR § 164.512(k)(2): to avert serious threats to the safety of the public if thePHI is given to authorized federal officials for the conduct of lawful intelligence, counterintelligence, or other national security activities. ***NOTE:*** *This disclosure requires accounting through the ROI Plus software. Also, a notification letter must be sent to the person to whom the health information pertains. The person has a right to know who received their information and what information was disclosed by VHA.*

(11) **Standing Written Request Letters:**

(a) Information disclosed in response to a standing written request letter is provided for the purpose of cooperating with a State governmental entity for reporting requirements. District Counsel will be consulted to determine if State laws would allow for standing written request letter to be implemented per the requirement s of 38 U.S.C 5701(f).

(b) Standing written request letters have been obtained to permit disclosure of IIHI by the facility to: (Delete or add to the list if you have more or you do not have these).

1. Law Enforcement: Law enforcement entities routinely require reporting from VHA records for suspected child abuse, suspected elder abuse, gunshot wounds, and other administrative actions (For example, suspension or revocation of a driver's license).

2. Public Health: Examples of public health reporting requiring a standing written request letter include:

a. Communicable diseases (For example, hepatitis, tuberculosis, sexually transmitted diseases, etc.),

b. Vital statistics (For example, deaths), and

c. Other State reporting requirements (For example, animal bites).

3. State and Other Public Registries (For example, State Cancer Registries). ***NOTE:*** *VHA may not disclose individually identifiable information to private registries without the prior written authorization of the individual to whom the information pertains)*.

4. Child Protective Services for reporting child abuse.

5. Coroner or Medical Examiner.

(c) Except for public health reporting requirement defined in VHA Directive 2013-008, Infectious Disease Reporting, all other disclosures are discretionary on behalf ofthe facility.

(d) Only the facility Privacy Officer may validate that a standing Written request letter meets the guidelines as defined in VHA Directive 1605.01paragaraph 21(b). A standing written request letter is good for a period of 3 years after which it must be renewed. A

copy of all standing written request letters must be maintained by the facility Privacy Officer for 5 years after the standing written request letter has expired.

(e) The facility Privacy Officer, or designee, is responsible for obtaining the standing written request letters for State agencies within the State locale. These standing letters will bemaintained, and records may be disclosed based on State law.

(f) Departments responsible for disclosing information pursuant to a valid standing written request letter must ensure an accounting of disclosures is maintained. The Departments will coordinate the disclosure with the Release of Information Department or Privacy Officer in order to have an appropriate process to account for the disclosure.

(g) If a standing letter is not in place the party requesting the IIHI must submit a written request under the authority of 5 U.S.C. 552a(b)(7) for the information. The request must be:

1. In writing.

2. Specify the portion of the record desired.

3. Specify the law enforcement activity or purpose for which the record is sought.

4. State that de-identified data could not reasonably be used.

5. Be signed by the head of the agency.

(12) **State Prescription Drug Monitoring Program (SPDMP):**

(a) The facility will disclose IIHI to a State Prescription Drug Monitoring Program (SPDMP) without the signed, written authorization of the Veteran for whom the medication was prescribed. Disclosure may be for the purpose of querying the SPDMP or reporting mandatory prescription information to theState (For example, batch reporting). ***NOTE:*** *Batch reporting is currently available and is handled by local IT and Pharmacy departments to ensure appropriate use and functionality of the process.*

(b) The ADPAC, Pharmacy Service, or designee is responsible for tracking the accounting of disclosures when querying the SPDMP.

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

(13) **De-identification of PHI:**

(a) Information is only considered de-identified if the methods outlined in VHA Directive 1605.01 Appendix A are followed. Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify the

individual and if VHA has no reasonable basis to believe it can be used to identify an individual. This is accomplished by either:

1. Having an expert with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small 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; and documents the methods and results of the analysis that justify such determination; or

2. All 18 identifiers listed in VHA Directive 1605.01 are removed.

(b) De-identified data is not PHI. Therefore, when data is appropriately de-identified, the HIPAA Privacy Rule, the Privacy Act, and other federal privacy regulations do not apply, and information may be disclosed under the FOIA.

(c) VA Directive 6511 must be followed prior to presenting at VA and non-VA conferences. Any questions concerning whether information is de-identified prior to disclosure, should be referred to the facility PO.

(14) **Research Activities: General**

(a) VA Research investigators must have appropriate legal authority to collect access or use individually identifiable information in a research study. The “need to know” in their official performance of their job duty does not cover all federal privacy regulations specific to research.

(b) The PO and the ISSO will serve in non-voting capacities on the Research and Development Committee pursuant to VHA Directive 1200.05 Requirements for the Protection of Human Subjects in Research.

(c) The PO will review all initial submissions of human subject research protocols, including exempt protocol submissions, for the use and/or disclosure of individually identifiable information and other privacy considerations prior to the convened IRB meeting at which the study is to be reviewed, except for those research projects approved by the VA Central IRB. It is expected that review submissions and approval process will be timely submitted by all parties involved. The ISSO will review all initial submissions of human subject research protocols for compliance with all applicable federal security requirements. Any privacy deficiencies will be communicated to the Principal Investigator. The PO and ISSO will provide a final written approval to the IRB. The PO’s final written summary must include approval of the HIPAA authorization and validation that the IRB appropriately approved the waiver of HIPAA. Authorization as appropriate prior to the use and/or disclosure of III by the researcher ortheir team.

1. Using the VA Form 10-250, VHA Research Protocol Privacy Review Checklist, the facility Privacy Officer will perform preliminary and final reviews of all initial submissions of human subject research protocols, including exempt protocol submissions in accordance with VHA Directive 1200.05 and 1605.03.

2. The facility PO and ISSO will review all continuing reviews of human subject protocols or proposed human subject protocol amendments impacting privacy or information security. VA Form 10-250 is only required if changes are made during the Continuing Review or Study Amendment, and this impacts the safeguarding and protection of the privacy and confidentiality of human subjects and study data.

(d) Facility research staff verifies the qualifications of VA researchers seeking to use and/or disclose III, (i.e., they have completed their mandatory privacy and security training) and ensures that the researchers take appropriate measures to protect the privacy of research subjects.

(15) **Research Activities: Use:**

(a) VA Research investigators may use III for reviews preparatory to VA research, provided that the information is being sought solely for purposes preparatory to research and that no PHI will be removed by the VA researcher. All other requirements related to the use of III for reviews preparatory to VA research are set forth in VHA Directive 1200.05(1), Requirements for Protection of Human Subjects Research must be followed.

(b) VA Research investigators may use PHI for VA-approved research if the facility PO has determined that:

1. A Research HIPAA authorization compliant with VHA Directive 1605.01 Para. 14 will be obtained for each research subject; or

2. IRB has approved a waiver of HIPAA authorization, in full or in part, and the IRBapproval has been appropriately documented as required by the HIPAA Privacy Rule and VHA Directive 1200.051); or

3. A Limited Data Set will be used and a valid DUA has been signed as required by the HIPAA Privacy Rule.

(c) If the researcher has not completed their study by the time of the expiration of the Research HIPAA authorization, the researcher can no longer use any of the information previously collected from the study subjects.

(d) PHI/III and other VA sensitive data for a VA-approved research study that is stored, collected, or maintained outside VA custody, either electronic or paper must have prior approval and safeguards in place to protect the data. The facility PO will work with the facility ISSO and CIO to ensure the appropriate safeguards are in place. See VA Handbook 6500 for further guidance.

(e) For certain sensitive research studies, A VA researcher may request a Certificate of Confidentiality from the National Institutes of Health (NIH) which, if granted could prevent the facility from being forced to disclose individually identifiable information on research subjects, by a court order/subpoena in any civil, criminal, administrative,

legislative, or other proceedings that are maintained in 34VA12, Veteran, Patient, Employee, and Volunteer Research and Development Project Records.

(16) **Research Activities: Disclosure:**

(a) For the facility to disclose protected health information to a non-VA researcher or other non-VA entity for research purposes, either for VA research purposes, or for non-VA research programs, there must be legal authority under all applicable federal privacy laws and regulations including 38 USC § 5701, the Privacy Act, HIPAA Privacy Rule and 38 USC § 7332. The applicable legal authority is as follows:

1. 38 USC § 5702: If the non-VA researcher or non-VA entity is requesting III, that may be disclosed under 38 USC § 5701, a written request stating records sought and purpose of the records that is dated and signed by the non-VA researcher is required. If VA is initiating the disclosure of information under 38 USC § 5701 for a research purpose, a written request from the non-VA researcher or non-VA entity is not required.

2. 38 USC § 5701: For purposes of disclosing records pertaining to any claim under any of the laws administrated by the Secretary for non-VA Research, a “federal” non-VA researcher may be provided name and address of individuals under 38 USC § 5701(b)(3). For a “non-federal” researcher or other entity, the researcher or entity must provide to VA the names and addresses of the individual whose claims information is being sought in order to obtain those individuals’ identifiable information.

3. 38 USC § 7332: The non-VA researcher to whom 38 USC § 7332 information (related to drug abuse, alcoholism, or alcohol abuse, infection with the human immunodeficiency virus, or sickle cell anemia) is disclosed must provide written assurance that the purpose of the data is to conduct scientific research and that no personnel involved in the study may identify, directly or indirectly, an individual patient or subject in any report of such research or otherwise disclose patient or subject identities in any manner. This assurance may be documented in the research protocol. In addition, the MCD based on input from the ACOS, Research and Development must determine that the non-VA researcher is qualified to conduct the research; has a research protocol that stipulates how the information will be maintained in a secure manner; and a written statement that the research protocol has been reviewed by an IRB who found that the individual’s rights are adequately protected and that the potential benefits of the research outweigh any potential risks to patient confidentiality. ***NOTE:*** *If a VA researcher plans to disclose 38 USC § 7332 information to an outside non-VA entity or use within a publication, this written assurance must also be obtained.*

4. Privacy Act of 1974: If an individual does not provide prior written consent for the disclosure of their record contained in a system of records (SOR), there must be a routine use under the applicable Privacy Act System of Records that permits the disclosure. (See 34VA12, Routine Use 19)

5. HIPAA Privacy Rule: A research HIPAA authorization compliant with VHA Directive 1605.01 Para. 14 will be obtained for each research subject; or the IRB has approved a waiver of HIPAA authorization and the IRB approval has been appropriately documented as required by the HIPAA Privacy Rule and VHA Directive 1200.05(1). ***NOTE:*** *A waiver of HIPAA authorization approved by the IRB does not affect or override the other legal requirements that must be met.*

(b) In the event of a security or privacy related incident, the facility ISSO and PO must be immediately notified upon discovery of the potential incident.

(c) A VA researcher must have appropriate legal authority to disclose individually identifiable information to a non-VA entity, including a research sponsor or an academic affiliate who is collaborating on this study. This disclosure authority is outlined in the written HIPAA authorization signed by the individual unless other legal authority exists, (For example, Court Order).

(d) Decedents' information may be disclosed to a source other than the researcher who has use of this data if the HIPAA Privacy Rule allows for disclosure to a non-VA entity. See your facility PO about any questions concerning disclosure authority.

(e) This facility may distribute a limited data set, information that excludes direct identifiers, but still contains potentially identifying information, without consent of the individual. A limited data set is only protected under the HIPAA Privacy Rule as the data is not considered identifiable for purposes of the Privacy Act and 38 USC 7332. Disclosure of a limited data set is dependent upon the receipt of a DUA, which must:

1. Establish the permitted uses and disclosures of the information.

2. Establish who is permitted to use or receive the data set.

3. Provide that the data set recipient:

a. Does not use for further disclose the information other than as permitted.

b. Uses appropriate safeguards to prevent improper use or disclosure of the information.

c. Reports to the facility/VHA any improper use or disclosure of which it becomes aware.

d. Ensures that any agents to whom it provides the data set agree to the same restrictions and conditions that apply to the data set recipient.

e. Does not identify the information or contact the individuals.

(f) A contracted entity involved in VA research is not a business associate of the covered entity and no BAA is required.

(g) A research disclosure made pursuant to a signed, written research HIPAA authorization to a non-VA entity (study monitor, sponsor, academic affiliate, or othernon-VA entities) who is not a research team member or contractor requires an accounting of disclosure to be maintained. The accounting of disclosure may be maintained concurrently or be created retrospectively from the VA researcher's files.See above Section B, Individual's Rights, Accounting of Disclosures.

(h) Facility will not disclose any personal information about VHA personnel engaged in animal research in response to a FOIA request if the FOIA Officer determines a risk to the facility or research personnel. ***NOTE:*** *Further guidance on Research requirements is available in VHA Directive 1605.01, VHA Directive 1200, and other applicable 1200 series handbooks.*

(17) **Logbooks:**

(a) Unnecessary collection of sensitive personal information (SPI) in physical logbooks is prohibited. VHA Directive 1605.01 Para. 2(g)(5) states, "VHA employees may maintain required electronic logbooks with appropriate safeguards in place. No paper logbooks may be kept unless there is a mandatory regulation that requires the physical logbook." While certain areas of the facility may be required to have certain paper or physical logbooks to meet regulatory requirements (For example, Laboratory, Radiology), most areas are not. And facility program and operations without regulatory requirements for paper or physical logbooks can and must maintain necessary logbooks electronically.

(b) Approved physical logbooks must be maintained no longer than their useful purposes and in accordance with VHA Records Control Schedule 10-1.

(c) Exceptions: Notwithstanding the above, a physical logbook is authorized in the following instances:

1. Emergency or computer contingence plan physical logbook used in a national disaster or when computers are down.

2. Facility Sign-in Roster: A sign-in roster is a temporary record that may be maintained for the purpose of personnel accountability such as training; or management of appointment scheduling. Sign-in rosters shall contain only the name and the time/date of access or arrival and purpose for visit (when in a non-clinical environment). Sign-in rosters will remain in direct unobstructed view of VHA staff. Sign-in rosters used for the purpose of appointment check-in shall contain only the name or signature and the time/date of access or arrival and must be destroyed at the completion of each business day using a VHA- approved destruction method. In clinical settings, supervisors shall implement measures to prevent patients from viewing the names and other SPI of patients who have previously signed in.

3. VA Form 4793, Visitor Register. Visitor registers may be used to record the name, destination, check in and checkout times of individuals when they are visiting an area. Registers may be placed, as necessary, at several locations throughout a facility.

At the end of the day the data must be destroyed or if there is a requirement to keep the data for a longer period of time the data must be transferred to an electronic tracking system or log, and the physical logbook pages must be shredded using a VHA approved method.

4. Security monitoring of restricted areas such as computer rooms. A sign in sheetin a computer room may be maintained for the purpose of personnel accountability. If there is a requirement to keep the data for longer than a day, then all security andNARA requirements must be met.

m. **FOIA:**

(1) **General Information:**

(a) The FOIA, Title 5 United States Code (U.S.C.)552, implemented by Title 38 Code of Federal Regulations (CFR), Sections 1.550-1.562 provides that any person has the right to obtain access to federal agency records, except to the extent that such records or portions of them are protected from public disclosure by one of the nine FOIA exemptions or by one of the three special law enforcement record exclusions.

(b) The FOIA requires disclosure of reasonably described VA records, or a reasonable segregable portion of the records, to any person upon written requestunless one or more of the nine exemptions apply to the records.

(c) A FOIA request may be made by any person (including foreign citizens), partnerships, corporations, associations, and foreign, State, or local governments with some exceptions. The following types of requests are not proper FOIA requests:

1. Requests for records by Federal agencies and their employees acting in their official capacity.

2. Requests for records by fugitives from justice seeking records related to their fugitive status.

(d) VHA administrative records not retrieved by name, social security number, or other identifier must be made available to the greatest extent possible in keeping withthe spirit and intent of the FOIA.

(e) Before releasing records in response to a FOIA request, the record must be reviewed by the FOIA Officer to determine if all or only portions of the record cannot be released, in accordance with the nine exemptions provided in the FOIA. The process of deleting portions of documents before releasing them is referred to as “redaction”.

(f) The FOIA mandates that all FOIA requests, absent unusual or exceptional circumstances, be processed within 20 business days of receipt.

(g) To foster ongoing communication and awareness on matters of significant importance to VA and VHA leadership, the facility FOIA Officer must provide notification

of substantial interest FOIA requests. A substantial interest FOIA Request is a request for information in which there has been or is likely to generate substantial public interest. This would include, but is not limited to, the following types of requests, regardless of the requester: (1) those related to a threat to the public health; (2) high profile local or national incidents or situations involving VA beneficiaries, employees or officials; and (3) incidents involving an alleged breach of the public trust (For example, waste, fraud or abuse). The FOIA Officer will notify VHSO Pentad upon receipt of such request via Outlook Mail identifying it as a substantial interest FOIA. The facility FOIA Officer will notify the VHA FOIA Office of all substantial interest FOIA requestsfollowing the current procedure set forth by the VHA FOIA Office.

(2) **Requests for Copies of Records:**

(a) Records or information customarily furnished to the public in the regular course of the performance of official duties (For example, information posted on VHSO Internet site) may be furnished without a written request. Employees may provide the website address to the requester to avoid having the individual submit a FOIA requestfor the records.

(b) Requests from individuals for information about themselves, which is retrieved by their names or other personal identifiers, need to be processed as previously outlined in section B., Individual Rights, Right of Access, unless the Privacy Act system of records maintaining the requested records has been exempted from a first party right of access. First party requests for records from such exempted Privacy Act systems of records will be processed under the FOIA.

(c) A FOIA request may be submitted through any mail service, by facsimile or electronically to an official FOIA mailbox established for the purpose of the receiving FOIA requests. Requests for VHSO records may be submitted to the facility's electronic FOIA mailbox at VHAFAVFOIA@VA.GOV or mailed to VHSO Privacy/FOIA Officer (013) at 1100 North College Avenue, Fayetteville, AR 72703.

(d) Requests for official VHA records under FOIA must be in writing and reasonably describe the records so that they may be located with a reasonable amount of effort. If a request, regardless of the method in which the request was received (i.e., mail, facsimile or e-mail), concerns documents involving a personal privacy interest or are protected by another confidentiality statute, the request must contain an image of the requester's handwritten signature. This procedure should not be waived for reasons of public interest, simplicity, or speed.

(e) Generally, the request does not have to be designated a FOIA request for the request to be processed as a FOIA request and the individual seeking the documents does not have to explain why access to official records is desired.

(3) **Processing an FOIA Request:**

(a) A request for records received at VHSO must be promptly stamped with the date the request was received and referred for action to the facility's FOIA Officer. Prompt

referral of any request for facility records to the facility FOIA Officer is required in order to ensure the below time limitations are met.

(b) All FOIA requests must be entered into the Department of Veterans Affairs' electronic FOIA tracking system.

(c) FOIA requests are sent to the facility's FOIA Officer will review the request to determine if the request is made in compliance with the FOIA and VA's regulations implementing the FOIA, if the requester is seeking a fee waiver or expedited processing, if the request meets the definition of a substantial interest FOIA request,and if the request was sent to the correct agency component.

(d) FOIA requests not submitted to the correct agency component will be promptly referred by the facility FOIA Officer to the correct component for processing.

(e) The facility FOIA Officer will address requests for fee waivers and expedited processing in accordance with the FOIA.

(f) Substantial interest FOIA request notifications will be completed in accordance with local and national procedures.

(g) The facility FOIA Officer shall charge for processing requests under the FOIA in accordance with the FOIA and VA implementing regulations.

(h) Within ten business days of receipt of the FOIA request, the facility FOIA Officer will acknowledge receipt of the request by sending the FOIA requester an acknowledgement letter that will contain the following information:

1. The date of the request.

2. The date the FOIA Officer received the FOIA request.

3. Description of the records sought.

4. The processing track type, (For example, simple, complex, or expedited).

5. Cut-off date of the records search.

6. The assigned FOIA request tracking number.

7. The name and contact information of the VHSO FOIA Officer handling the request.

(i) A reasonable search for records responsive to the FOIA request will be conducted by the VHSO employees. All records responsive to a FOIA request will be forwarded to the facility's FOIA Officer for processing.

(j) In instances where the FOIA requester fails to provide enough information to locate the requested records, the FOIA Officer will seek clarification from the FOIA requester.

(k) In unusual circumstances, the facility FOIA Officer may extend the 20-business daytime limit to process FOIA request an extra 10 business days. The FOIA Officer will notify the requester of the unusual circumstances, that a time extension has been taken, and the date which a response is expected to be issued. If the extension is more than 10 business days, the FOIA Officer will inform the requester of this in writing and provide the requester an opportunity to narrow the scope of the request or arrange foran alternate timeframe.

(l) After making a release determination, the facility FOIA Officer will issue an initial agency decision (IAD) to the requester. The IAD letter must contain the following information:

1. Date of the request.

2. Date the FOIA Officer received the request.

3. Clearly re-state the requested records, (description of records sought).

4. The assigned FOIA request tracking number.

5. The procedural history of the request

6. The cut-off date of the record search.

7. The exemption(s) cited when information is being redacted or withheld.

8. The type of information being redacted or withheld (i.e. name, SSN, address, etc.).

9. If any adverse determinations are made, the right to appeal to the Office of General Counsel (OGC).

(m) IADs for FOIA requests denied in whole or part must be signed by the MCD or PO or designee if signature authority has been granted by the Medical Center.

(n) FOIA administrative case files will be maintained in accordance with RCS 10-1, and the National Archives and Records Administration (NARA) General Records Schedule and contain the following information:

1. Copy of the FOIA request.

2. Evidence demonstrating that the FOIA Officer conducted a thorough search for responsive records.

3. Un-redacted copies of responsive records.

4. Redacted copies of responsive records sent to the FOIA requestor.

5. Copies of all correspondence, including the signed IAD letter, and contact with requesters and in the case of exemption 4, the submitter, to include, but not limited to emails and letters concerning acknowledgement, fees, scope, clarification,pre-disclosure notification, notice of intent and the initial agency decision. ***NOTE:*** *Refer to VHA Directive 1605.01 Privacy and Release of Information paragraph 32, and Freedom of Information Act for additional information on processing FOIArequests.*

(4) **Coordination of Releases with Regional Counsel and VHA FOIA Officer:**

(a) The facility FOIA Officer will consult with Regional Counsel, VISN, and the VHA FOIA Office concerning FOIA legal requirements and the handling of specific FOIA requests.

(b) In any case where a FOIA request involves matters or subjects involved in ongoing or anticipated litigation, administrative proceedings, or criminal or civil investigation, health care facility personnel must coordinate the facility's response to the FOIA request with the local Office of Chief Counsel, Continental District.

(c) If a request involves matters pertaining to ongoing litigation, the Chief Counsel must be informed of the request to ensure coordination of the VA's position in the litigation with any release of documents.

(5) **Annual Report of Compliance with FOIA**. The FOIA requires each agency to complete an annual FOIA report. The facility FOIA Officer must ensure that all requests for the annual FOIA report are properly entered into the VA's electronic FOIA tracking system to allow for an accurate reporting on the annual FOIA report.

5. **DEFINITIONS**

a. **Access.** Is the obtaining or using of information, electronically, on paper, or through other medium, for the purpose of performing an official function.

b. **Availability.** Availability means that data or information is accessible and useable upon demand by an authorized person.

c. **Business Associate.** Business associate is an entity, including an individual, company, 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.

d. **Compelling Business Need.** A compelling business need is one that requires the capture of SPI in logbook form to meet a policy, regulatory, accreditation or statutory requirement. Additionally, compelling business needs may support reasonable and appropriate business operations, patient safety or quality improvement efforts, or other

prudent and important health care operations needs such as the board certification of clinical staff including residents and trainees.

e. **Computer Matching.** Computer matching describes the computerizedcomparison of records from two or more automated systems of records.

f. **Confidentiality.** Confidentiality means that property, data, or information is not made available or disclosed to unauthorized persons or processes.

g. **De-identified Information.** De-identified information is heath information that does not identify an individual and provides no reasonable basis to believe that the information can be used to identify the individual because the 18 Patient Identifiers described in the HIPAA Privacy Rule have been removed. De-identified information isno longer covered by the Privacy Act, 38 U.S.C. § 5701, 38 U.S.C. § 7332, or the HIPAA Privacy Rule.

h. **Disclosure.** Disclosure means the release, transfer, provision of, access to, or divulging in any other manner, of information outside the entity holding the information.

i. **Electronic Media.**

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media includes:

(a) The Internet (wide-open).

(b) Extranet (using internet technology to link a business with information accessible only to collaborating parties).

(c) Leased lines.

(d) Dial-up lines.

(e) Private networks.

(3) The physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

j. **Health Care Operations.** Health care operations means 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:

(a) Outcome's 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.

(b) Patient safety activities (as defined in 42 CFR 3.20).

(2) Reviewing the competence or qualifications of health care professionals, including:

(a) Evaluating practitioner and provider performance and health plan performance.

(b) 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.

(c) 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 auditingfunctions, 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.

(6) Business management and general administrative activities of the entity, including, but not limited to:

(a) Management activities relating to implementation of and compliance with the HIPAA requirements.

(b) Customer service, including the provision of data analyses for policy holders,plan sponsors, or other customers, provided that protected health information is notdisclosed to such policy holder, plan sponsor, or customer.

(c) Resolution of internal grievances; creating de-identified health information or a limited data set.

(d) Fundraising for the benefit of the covered entity.

k. **Health Information.** Health Information is any 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:

(1) The past, present, or future physical or mental health or condition of anindividual.

(2) The provision of health care to an individual; or payment for the provision of health care to an individual.

(3) This encompasses information pertaining to examination, medical history, diagnosis, and findings or treatment, including laboratory examinations, X-rays, microscopic slides, photographs, and prescriptions.

l. **Individual.** An individual means the person who is the subject of protected health information.

m. **Individually Identifiable Information.** Individually Identifiable Information (III) 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.

n. **Individually identifiable Health Information** Individually Identified 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.

(2) Relates to the past, present, or future physical or mental condition of anindividual and provision of, or payment for, health care.

(3) Identifies the individual or provides a reasonable basis to believe it can be usedto identify the individual.

o. **Limited Data Set.** Limited Data Set is protected health information from which certain specified direct identifiers of the individuals, their relatives, household members, and employers have been removed.

(1) These identifiers include:

(a) Name.

(b) Address (other than town or city, state, or zip code).

(c) Phone number.

(d) Fax number.

(e) Email address.

(f) Social Security number.

(g) Medical record number.

(h) Health plan number.

(i) Account number.

(j) Certificate and/or license numbers.

(k) Vehicle identification.

(l) Device identifiers.

(m) Web universal resource locators (URL).

(n) Internet protocol (IP) address numbers.

(o) Biometric identifiers.

(p) Full–face photographic images.

(2) 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.

(3) Thus, a Limited Data Set is not De-identified Information, and is covered by the HIPAA Privacy Rule.

(4) A Limited Data Set may be used and disclosed for research, healthcare operations, and public health purposes pursuant to a Data Use Agreement.

p. **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 38 U.S.C. 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 Rule's de-identification standards are removed.

q. **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 Rule.

r. **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. It 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.*

s. **Physical Logbook:** A physical logbook is any written (i.e., not electronic) recordof activities or events comprised of data **(**which may uniquely identify an individual or contain SPI**)** that is maintained over a period of time for the purpose of monitoring an activity, tracking information or creating a historical record.

(1) Examples of physical logbooks:

(a) Respiratory therapy logs.

(b) Laboratory logs.

(c) Autopsy logs.

(d) Facility access logs.

(e) Wound care logs.

(f) Logs of cases cleared.

(g) Printouts of Excel spreadsheets.

(h) Access data base printouts.

(2) Examples of items which are not physical logbooks:

(a) Any electronic file.

(b) A list of codes only, such as study identification codes that do not identify an individual.

(c) Paper documents required by health care providers for the care of individual patients (e.g., index cards).

(d) Police pocket notecards, with incident information and daily activities

(e) Paper sign-out records (hand-offs) with information on multiple patients constituting a team or panel and required to transfer the care of patients betweenhealth care providers.

(f) A contact list of employees' names, work phone numbers or work addresses.

(g) Work process list.

t. **Personally Identifiable Information**. Personally Identifiable information (PII) is any information which 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".*

u. **Protected Health Information.** The HIPAA Privacy Rule defines Protected Health Information (PHI) as Individually Identifiable Health Information that is 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 confidentially statutes. In addition, 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.*

v. **Right of Access.** Right of access is an individual's right to have access to (e.g., look at, view) or obtain a copy of records pertaining to the individual that contain individually identifiable information.

w. **Sensitive Personal Information.**

(1) Sensitive Personal Information (SPI), with respect to an individual, means any information about the individual maintained by VA, including the following:

(a) Education

(b) Financial transactions

(c) Medical History

(d) Criminal or employment history

(e) Information that can be used to distinguish or trace the individual's identity:

1. Name

2. Social Security Number

3. Date and place of birth

4. Mother's maiden name

5. Biometric records.

(2) SPI is a subset of VA Sensitive Information/Data.

(3) The term “Sensitive Personal Information” is synonymous and interchangeable with “Personally Identifiable Information”.

x. **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.

y. **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 personal identifier such as the name of the individual, number, symbol, or other unique retriever assigned to the individual.

z. **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 providers relating to a patient, and the referral of a patient for health care from one health care provider to another.

aa. **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 or 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, 38 U.S.C § 5701, or 38 U.S.C. § 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 Identifier 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 (For example, A2222) is not a unique identifier; therefore, inclusion of this number by itself does not make by itself does not make the information identifiable or sensitive.*

bb. **Use.** Use is the sharing, employment, application, utilization examination, or analysis of information within VHA.

cc. **VA Sensitive Information Data.** VA Sensitive Information Data is all department information and/or data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes not only information that identifies an individual, but also other information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.

dd. **Workforce.** Workforce means on-site or remotely located employees, contractors, students, WOC, volunteers, and any other appointed workforce members.

6. **REFERENCES**

a. Public Law 104-191, Health Insurance Portability and Accountability Act of 1996 (HIPAA).

b. Public Law 111-5, American Recovery and Reinvestment Act of 2009, Title XIII, 13001, Health Information Technology for Economic and Clinical Health Act.

c. Title 5 United States Code (U.S.C.) 552, Freedom of Information Act.

d. Title 5 United States Code (U.S.C.) 552A, Privacy Act of 1974.

e. Title 5 United States Code (U.S.C.) 7114 (b)(4), Representation rights and duties.

f. Title 38 United States Code (U.S.C.) 5701, Confidential Nature of Claims.

g. Title 38 United States Code (U.S.C.) 5702, Furnishing of records.

h. Title 38 United States Code (U.S.C.) 5705, Confidentiality of Healthcare Quality Assurance Review Records.

i. Title 38 United States Code (U.S.C.) 7332, Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Medical Records.

j. Title 38 Unites States Code (U.S.C.) 1.576(b)(7), General policies, conditions of disclosure, accounting of certain disclosures and definitions.

k. Title 38 Unites States Code (U.S.C.) 1.577(f), Access to records.

l. Title 38 Unites States Code (U.S.C.) 1.579, Amendment of records.

m. Title 38 Code of Federal Regulations (C.F.R.) 1 .582 as published by Final Rule on June 13, 2003, in Federal Register Volume 68, Number 114 on pages 35297 through 35299.

n. Title 38 Code of Federal Regulations (C.F.R.) 14.800 – 14.810, Touhyregulations.

o. Title 42 Code of Federal Regulations (C.F.R.) 3.20, Patient Safety Organizations and Patient Safety Work Product.

p. Title 45 Code of Federal Regulations (C.F.R.) parts 160 and 164, Standards for Privacy of Individually Identifiable Health Information.

q. VA Directive 5021, Employee/Management Relations, dated April 15, 2002.

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

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

t. VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, dated March 12, 2019.

u. VA Handbook 6500.6, Contract Security, dated March 12, 2010.

v. VA Directive 6502, VA Enterprise Privacy Program, dated May 5, 2008.

w. VA Handbook 6508.1, Procedures for Privacy Threshold Analysis and Privacy Impact Assessment dated July 30, 2015.

x. VA Directive 6511, Presentations Displaying Personally Identifiable Information, dated January 7, 2011.

y. VA Directive 6371, Destruction of Temporary Paper Records, dated April 8, 2014.

z. VA Directive 6609, Mailing of Sensitive Personal Information, dated May 20,2011.

aa. VHA Directive 1078, Privacy of Persons Regarding Photographs, DigitalImages, and Video or Audio Recordings, dated November 29, 2021.

bb. VHA Directive 1200.01(1), Research and Development Committee, dated January 24, 2019.

cc. VHA Directive 1200.05(1), Requirements for the Protection of Human Subjects in Research, dated January 7, 2019.

dd. VHA Handbook 1200.12, Use of Data and Data Repositories in VHA Research, dated March 9, 2009.

ee. VHA Directive 1605, VHA Privacy Program, dated September 1, 2017.

ff. VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016.

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

hh. VHA Directive 1605.03(1), Privacy Compliance Assurance Program and Privacy/Freedom of Information Act (FOIA) Continuous Readiness Review and Remediation, dated September 19, 2019.

ii. VHA Handbook 1605.04, Notice of Privacy Practices, September 6, 2015.

jj. VHA Handbook 1605.05, Business Associate Agreements, November 17, 2020.

kk. VHA Directive 1615, Mandated Utilization of Release of Information (ROI) Plus Software, dated March 23, 2022.

ll. VHA Directive 1935, VHA Freedom of Information Act Program, dated February5, 2018.

mm. VHA Notice of Privacy Practices, 1B 10-163, dated September 30, 2019.

nn. VHA Records Control Schedule 10-1, dated January 2021.

oo. VA form 10-0483, Acknowledgement of the Notice of Privacy Practices.

pp. 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.

qq. VA form 10-5345, Request for and Authorization to Release Health Information.

rr. VA form 10-5345a, Individuals' Request for a Copy of Their Own Health Information.

ss. VA form 4793, Visitor Register.

7. RECORDS CONTROL

All records will be maintained and inventoried in accordance with MCP 04-03 and RCS 10-1. If applicable, records will be inventoried on the Privacy Office record file and inventory plan.

8. RESCISSION

VHSO MCM 17-001-31, Privacy Policy, dated February 26, 2018

9. REVIEW

This MCP must be reviewed annually and at recertification, to include when there are changes to the governing document (For example, national policy or a health care accreditation body mandate).

10. RECERTIFICATION

This MCP is scheduled for recertification on or before the last working day of February 2028. This MCP will continue to serve as local policy until it is recertified or rescinded. In the event of contradiction with national policy, the national policy supersedes and controls.

11. SIGNATORY AUTHORITY

GEORGE VELEZ Digitally signed by GEORGE VELEZ
Date: 2023.02.08 12:17:49 -06'00'

George Velez, DHA, MBA, FACHE
Medical Center Director

NOTE: The signature remains valid until rescinded by an appropriate administrative action.

DISTRIBUTION: Via Intranet.

APPENDIX A

SPECIAL MAIL HANDLING

1. Access to these records is limited to:

AUTHORIZED PERSONS ONLY

2. Information may not be disclosed from this file unless permitted pursuant to 38 CFR 1.500-1.599.

3. These records may not be altered or destroyed except as authorized by 38 CFR 1.579.

4. The Privacy Act contains provisions for criminal penalties for knowingly and willfully disclosing information from this file unless properly authorized to do so. The HIPAA contains similar provisions.

(This notice should be placed inside of the envelope or package)

SPECIAL ATTENTION MAIL