VETERANS BENEFITS ADMINISTRATION PRIVACY PROGRAM – RESOURCE GUIDE

Version 1

INTRODUCTION

The goal of this "Privacy Program Resource Guide" is to help Privacy Officers gain the skills, knowledge, and support needed to be highly effective in their positions. To be successful, Privacy Officers in the Veterans Benefits Administration (VBA) must know Standard Operating Procedure (SOP), organizational structure, computer applications, available resources, and everyday terminology unique to VBA. Privacy Officers must know how to access and use the wide realm of data at hand to manage our specialized program area and be able to embrace changing roles and grow with the environment.

The intent is to keep the guide current and updated to reflect the latest directives, policies, and guidance that relate to the needs of VBA's Privacy Program.

CONTENTS

VBA PRIVACY OFFICE

Implements VA Privacy policies at VBA Program Offices, business lines and regional offices to ensure federal regulatory requirements, VA policies and procedures are followed as it relates to the Privacy Act of 1974.

VBA Chief Privacy Officer Rochelle Foxworth
VBA Privacy Office Mailbox – privacy.vbavaco@va.gov

Other Privacy Stakeholders:

VA Privacy Service Office	• Develop and implement policy and regulations. • Develop and provide privacy training. • Address questions and provide guidance. • Provide privacy subject matter experts. • Provide resource and reference materials. • Release of Information (ROI) plus software
Data Breach Response Service	• Handle all Privacy and Security related events on a national level. • Determines along with the National Data Breach Core Team (DBCT) on complex issues and whether individuals are offered credit protection services. • Required by law to report quarterly to Congress on data breaches within VA
VBA Freedom of Information Act (FOIA) Office	• Responsible for responding to VBA FOIA requests. • Provides guidance on VBA FOIA requests. • Develop and provide training VBA FOIA Officers • Submits annual FOIA report to Congress. • Monitor FOIAXpress software
Centralized Support Division	• Responsible for processing and responding to VBA Privacy Act and FOIA requests

Back to top

VBA PRIVACY OFFICER RESPONSIBILITIES

VBA CHIEF PRIVACY OFFICER

The VBA Chief Privacy Officer shall:

Provide guidance to VBA *Program Office (PO) and Regional Office (RO) Privacy Officers, as appropriate, to ensure that policies and practices at those facilities adhere to federal privacy laws and VA and Administration policies and procedures.

Provide instruction regarding responsibilities and requirements for implementation of the privacy program within VBA Program Offices/Regional Offices and report the status to the Privacy Service at least quarterly.

Monitor and administer VBA privacy training and awareness to VBA Lines of Business, Program Office, and Regional Office Privacy Officers by providing:

- General privacy and Health Insurance Portability and Accountability Act (HIPAA) privacy training, as appropriate; and
- VA National Rules of Behavior training

As appropriate, coordinate with VBA Lines of Business, Program Office and Regional Office Privacy Officers, and Information System Owners and System Managers to ensure that all data and associated risks are identified and documented in Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) submissions to the Privacy Service; and

Work with the VA Privacy Service and VA Enterprise Risk Management (ERM) to ensure VBA Lines of Business, Program Office, and Regional Office Privacy Officers are available to assist in compliance monitoring assessments.

** Program Offices refer to VBA Central Office Lines of Business and Staff Offices. Some Lines of Business exist within VBA Regional Offices that are under the jurisdiction of the Executive Director.*

VBA CENTRAL OFFICE PRIVACY OFFICER

The VBA Central Office Privacy Officer shall:

- Be aligned under the Director for all privacy-related issues.
- Self-assign and complete the following Talent Management System courses:
    - VA Privacy Officer Competency Model Training within TMS: Privacy Webinar Series: Getting Started as Privacy Officer
    - VA Privacy Officer Professionalization Training: Privacy Events
    - VA Privacy Officer Professionalization Training: Privacy

Back to top

Threshold Analysis (PTA)

- VA Privacy Officer Professionalization Training: Privacy Impact Assessment (PIA)
- Privacy Webinar Series: Completing the Facility Self- Assessment (FSA)
- Privacy Webinar Series: The System of Records Notice
- Privacy Webinar Series: Federal Privacy Fundamentals and Implementation
- Privacy Webinar Series: Contract Reviews (OnDemand)
- Privacy Webinar Series: Implementing Privacy During the eMASS Workflows
- Privacy Webinar Series: Privacy Controls Background
- Privacy Webinar Series: Being a VA Business Associate

- Establish a Privacy and Security Events Tracking System (PSETS) account with the Data Breach Response Service (DBRS).
- Receive all request for records and determine whether to process as a Privacy Act (PA) request and then take appropriate subsequent action.
- Perform all privacy duties and responsibilities as designated by the VBA Line of Business or Program Office.
- Knowledgeable of all laws and VA regulations concerning the release of information under Privacy Act of 1974.
- Perform all privacy duties and responsibilities as designated by the VBA Privacy Officer.
- Knowledgeable of all laws and VA regulations concerning the release of information under the Privacy Act.
- Disclose information based on the legal authority.
- Provide guidance to employees on all privacy-related matters.
- Provide assistance in the development and update of privacy policies within he VBA Line of Business or Program Office.
- Coordinate with VBA Privacy Officers to verify that a System of Record Notice (SORN) has been published for all information systems subject to the Privacy Act.
- The Privacy Officer shall be knowledgeable of the Data Breach Response process as outlined in VA Handbook 6500.2.
- Report all actual or suspected breaches of privacy of Personally Identifiable Information (PII) observed or received to the VA Cyber Security Operations Center (VA-CSOC) and the VA Data Breach Response Service (DBRS) within one hour as designated by the VA Privacy Office.
- Initiate investigations the same day they are reported into the Privacy and Security Events Tracking System (PSETS).
- Using the template letters provided by DBRS, notify the subject of the investigation within 60 days of notifying DBRS.
- Perform walk-through inspections once a quarter at VBA Central Office located at 1800 G Street, NW, Washington, DC 20006. The Privacy Officer shall

Back to top

document their findings in writing and provide a copy to the VBA Line of Business or Program Office executive leadership team.

- All local produced briefing/slide decks are to be submitted to the Privacy Officer for review one (1) week prior to the briefing. The Privacy Officer shall have three (3) business days to review the briefing/slide decks. The Privacy Officer and the presenter shall complete their portion of the VA Form 0897 Presenter Certification. For further guidance, see Presentations containing PII SOPs.
- Perform Privacy Self-Assessments in accordance with the Privacy Self-Assessment Program SOP.
- Perform privacy self-assessments using the Facility Self-Assessment software tool. Complete the appropriate section quarterly.
- Be involved in operational/strategic planning to provide the privacy perspective for PO or RO decision-makers.
- Be made aware of systems development or modifications that may require a PIA be completed.
- Review all contracts to ensure compliance with VA Directive 6500.6 Appendix A VA Publications Home Page using the provided checklist.
- Ensure the applicable sections of VA Handbook 6500.6 Appendix C VA Publications Home Page is included in the statement-of-work if VA sensitive information is stored, generated, transmitted, or exchanged by or with a vendor.
- Provide privacy training to all new employees annually.
- Provide continuous privacy training to VBA Line of Business or Program Office workforce.
- Monitor, in conjunction with the TMS Training Coordinator and Contracting Officer's Representative (COR), on a continuing basis, for employees, Veterans Service Organizations (VSO) and contractors, to include:
- TMS compliance:
    - Ensure VA Privacy and Information Security Awareness and Rules of Behavior (ROB), TMS course # VA10176 is completed by all new employees (including contractors/subcontractors) within 30 days of assignment to the VBA Line of Business or Program Office and monitor annual compliance requirement.
    - The Privacy Officer shall receive a monthly report on the last day of the month from the Training Coordinator.
    - Ensure employees with access to the Compensation and Pension Records Interchange (CAPRI) system completes the Privacy and HIPPA Training (VA 10203).
- Continuously monitor all aspects of the VBA Line of Business or Program Office Privacy Program to include but not limited to:
- Quarterly Privacy Walk-throughs to include but not limited to workstation privacy compliance.
- Auditory compliance
- Ensure no paper logbooks are kept unless there is a mandatory regulation that requires the physical logbook. Only electronic systems or one-time use slips shall be used.

Back to top

VBA REGIONAL OFFICE PRIVACY OFFICER

The duties of a VBA Privacy Officer include:

- Privacy Officer will be aligned under the Regional Office Director for all privacy related issues.
- Establish a Privacy and Security Events Tracking System (PSETS) account with Data Breach Response Service (DBRS).
- Perform all privacy duties and responsibilities as designated by the VBA Privacy Officer.
- Process Privacy Act requests.
- Knowledgeable of all laws and VA regulations concerning the release of information under the PA.
- Disclose information based on the legal authority.
- Provide guidance to employees on all privacy-related matters.
- The Privacy Officer shall be knowledgeable of the Data Breach Response process as outlined in VA Handbook 6500.2, *Management of Security and Privacy Incidents.*
- Report all actual or suspected breaches of privacy/PII, observed or received, to the VA Cyber Security Operations Center (VA-CSOC) and DBRS within one hour, as directed by the VA Privacy Service.
- Initiate investigations the same day they are reported into the Privacy and Security Events Tracking System (PSETS).
- Using the template letters provided by DBRS, notify the affected parties within 60 days of notifying DBRS.
- Privacy Officer shall perform annual walk-through inspections of their assigned Regional Office.
- Process PRAD Facility Self-Assessment, utilizing the Facility Self-Assessment software tool, located at Home (va.gov). Complete appropriate sections quarterly.
- Review all contracts to ensure compliance with VA Directive 6500.6 Appendix A, Checklist for Information Security, utilizing the provided checklist.
- Ensure the applicable sections of VA Handbook 6500.6 Appendix C is included in the statement-of-work and/or contract if VA sensitive information is stored, generated, transmitted, or exchanged by or with a vendor.
- Provide Privacy training to all new employees within 30 days of starting work.
- Provide activities to foster privacy awareness throughout the year. For example, send emails, distribute privacy posters, etc.
- Monitor all aspects of the RO Privacy Program on a continuing basis, for employees, VSOs and Contractors, to include:
    - Privacy walk-throughs
    - New Employee Orientation (NEO) Privacy training
    - Employee compliance
    - TMS compliance (TMS courses 10176 and 10203)
    - Auditory compliance

Back to top

- Ensure no paper logbooks are kept unless there is a mandatory regulation that requires the use of a physical logbook, per VAIQ # 7092263, *Prohibition of Written Logbooks*. Only electronic systems or one-time use slips shall be used.

Some duties may differ for CSD Privacy Officers.

For a complete listing of Privacy Officer responsibilities see https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=809&FType=2 (Duties of Privacy Officers).

NOTICE OF PRIVACY PRACTICES (NOPP)

The goal of the VBA NOPP is to:

1. Inform individuals of the ways in which VBA may use and disclose their Personal information with or without their authorization.
2. Notify individuals of their rights to access, inspect, request an amendment, and/or restriction of their claims information; and
3. Inform individuals of VBA's legal obligations to maintain the privacy of their Personal information.

The VBA NOPP will effectively communicate to the recipients VBA's legal requirements to:

1. Ensure the privacy of PII.
2. Provide notice of VBA's legal obligations and privacy practices with respect to their PII; and
3. Communicate VBA's responsibility to follow the terms of the VBA Notice of Privacy Practices that are currently in effect.

INDIVIDUAL PRIVACY RIGHTS

- **RIGHT TO A NOTICE OF PRIVACY PRACTICES –** VA must notify individuals in writing how VA may use or disclose their health information, how they may exercise their privacy rights and how they may submit privacy complaints (HIPAA Privacy Rule).

- **RIGHT TO REQUEST AMENDMENT –** An individual has the right to request an amendment to any VA information retrieved under his/her unique identifier. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely, as well as the reason for this belief. The request must be signed. Note: There are a few exceptions under a Privacy Act system of records where an individual may not request an amendment. For example, VA police records. Due to required timeframes, it is important to follow the guidance outlined in the section on amendments. (HIPAA Privacy Rule and Privacy Act)

- **RIGHT TO ACCESS RECORDS –** Individuals have the right to request and receive copies of their individual records retrieved by their unique identifier. Denials of requests should be minimal. An example would be a request for police investigative records and the investigation is still open. Failure to provide records can result in an appeal to the Office of General Counsel. (HIPAA Privacy Rule and Privacy Act)

- **RIGHT TO CONFIDENTIAL COMMUNICATIONS –** An individual has the right to request and receive communications confidentially by an alternative means (in person) or at an alternative location (address other than the individual's permanent address).

- **RIGHT TO AN ACCOUNTING OF DISCLOSURES –** An individual may request a list of all disclosures of information, both written and oral, from records pertaining to the individual. However, it has been determined that VBA only need to maintain an accounting of written disclosures. The PO or RO is required to keep an accurate accounting for each disclosure of a record to any person or to another agency. Accountings are not required when the information being requested is for the performance of official VA employee duties. Sensitive Patient Access Reports (SPAR) are not considered an accounting of disclosure. However, an accounting of disclosure is required if a SPAR is requested and disclosed. (HIPAA Privacy Rule and Privacy Act)

RIGHT TO FILE A PRIVACY COMPLAINT – Veterans, their dependent or representative may file a written complaint with the PO or RO Privacy Officer, the Office of Inspector General (OIG), Department of Health and Human Services, Office for Civil Rights. The facility must respond in writing to the complainant. All privacy complaints/incidents must be entered into the Privacy Security Event Tracking System (PSETS) within one (1) hour of when the Privacy Officer becomes aware. (HIPAA Privacy Rule)

FACILITY SELF ASSESSMENTS

It is recommended that VBA Privacy Officers establish local privacy policy. The components are listed in VA Directive 6509.

All VBA Privacy Officers are required to complete a quarterly facility self-assessment, evaluating specific sections of the facility privacy program each quarter as outlined in the VA Directive 6509. Assessments are due on a quarterly basis, no later than the last business day of each quarter (December, March, June, and September of each fiscal year). You can find the templates for the facility self-assessment on **VBA's Privacy Share point site**. Privacy - Home (sharepoint.com)

MANDATORY EMPLOYEE PRIVACY TRAINING

All VA employees are required to complete privacy training within 30 days of being hired and before they have access to PHI/ PII. Training must be completed annually thereafter on the anniversary date of when the training was last completed.

Completion of the TMS VA Privacy and Information Security Awareness and Rules of Behavior (VA10176) will satisfy the annual information security and general privacy awareness requirement for VA employees prior to having network access (VA computer systems). This course has automatically been assigned to all VA employee training plans. This combined course will satisfy VA employee privacy requirements who do not have access to **PHI/PII**.

If employees have access to protected health Information **PHI/PII** they are required to take the additional TMS VHA Privacy and HIPAA Training (VA10203) requirement. This training can be accessed in TMS whether on a VA computer or from a personal computer.

Volunteers, VA Contractors, Without Compensation (WOC) are considered employees.

The TMS Mandatory Training for Trainees (MTT) (3185966-new; 3192008-refresher) course is a full and acceptable substitute for ANY other national mandatory training modules, including Privacy and Security individual modules for health professional trainees. This course constitutes the minimum curriculum necessary for a trainee, e.g., resident, to train safely and effectively in VA. Your local VA office may have additional requirements.

VA Talent Management System:
https://logon.iam.va.gov/affwebservices/public/saml2sso?SPID=https://www.successfactors.com/VAHCM03.

RECOMMENDED PRIVACY OFFICER TRAINING

- VA Privacy Officer Competency Model Training within TMS: Privacy Webinar Series: Getting Started as Privacy Officer
- VA Privacy Officer Professionalization Training: Privacy Events
- VA Privacy Officer Professionalization Training: Privacy Threshold Analysis
- Privacy Webinar Series: Completing the Facility Self-Assessment (FSA)
- Privacy Webinar Series: The System of Records Notice
- Privacy Webinar Series: Federal Privacy Fundamentals and Implementation
- Privacy Webinar Series: Contract Reviews
- Privacy Webinar Series: Implementing Privacy During the eMASS Workflows
- Privacy Webinar Series: Privacy Controls Background
- Privacy Webinar Series: Being a VA Business Associate

**These trainings can be found in TMS or VA On Demand.*

PRIVACY ACT

Privacy Act.
The Privacy Act, passed in 1974, gives individuals a greater say in the way records about them are kept and eliminates needless intrusions on personal privacy by eliminating extraneous records. The Office of Management and Budget (OMB) has lead responsibility for developing guidelines and administering the Act.

What is protected under the Privacy Act? Records about an individual under the control of an executive branch agency that are retrieved by a personal identifier. These records are considered part of a "system of records" and are protected by the Privacy Act. The basic purpose of the Privacy Act is to help protect the privacy of individual citizens.

Difference Between FOIA and Privacy Act.
FOIA is an information access law, whereas the PA is an information protection law with limited access provisions. Anyone may submit an FOIA request for any type of record, but a PA request may only be made by the individual (or his or her legally authorized representative) covered by the requested records. Regardless, VA policy requires that the request be processed under the law that provides the greatest amount of access.

The PA applies to any VA records about an individual which are retrieved by the individual's name or other identifier, regardless, of the storage media such as paper or computer disk.

Veterans have the right to access their VA records that may contain their name and/or other unique identifiers, and the right to have VBA amend those records when the records are not accurate, timely, complete, and relevant.

The PA prohibits disclosure of any records about an individual which are retrieved by that individual's name and/or other unique identifier, unless disclosure is specifically authorized by the PA. 5 U.S.C. § 552a.

a) **NOTE**: If another confidentiality statute also applies to the records, that statute also must authorize the specific disclosure before VA may disclose the record.

VA is required to meet certain "fair information practice standards" in the collection, maintenance and use and disclosure of the information protected by the PA.
The PA applies to records about an individual who is a United States citizen and whose records are retrieved by the name or other personal identifier of the individual. A record is information contained in a document derived from a document or database associated with a particular individual. Besides United States citizens, the Act also applies to aliens lawfully admitted to permanent residence in the United States.

Policy:
Information may be disclosed to a Veteran or their duly authorized representative as to matters concerning themself alone. If the Veteran is deceased, matters concerning them may be disclosed to their spouse, children, or next of kin if such disclosure will not be injurious to the physical or mental health of the person on whose behalf information is sought or cause repugnance or resentment toward the decedent.

VBA utilizes the Centralized Support Division (CSD) to process most of its FOIA/Privacy Act requests. The Regional Office FOIA/Privacy Officer will be responsible for processing the requests that are excluded from the CSD.

INDIVIDUAL RIGHTS OF ACCESS

Access.
Veterans have the right to access and/or view and obtain a copy of their own information, including PII, contained in a VBA System of Records.

Amend.
An individual has the right to request an amendment to any information contained in a VA System of Records, as provided in 38 CFR, Section 1.579. Unless authority to deny the request is present, VBA must grant the individual's right to correct or amend his/her information.

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

The written amendment request will be routed to the RO Privacy Officer. Amendment requests are to be maintained by the RO Privacy Officer.

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

Accounting of Disclosures.
Veterans have the right to an accounting of prior disclosures of their PII. They may request a list of all prior disclosures of information, both written and oral, from records pertaining to them, subject to the provisions of 38 CFR, Section 1.576(c).

PROCESSING PRIVACY ACT REQUESTS

Written Requests. VBA requires that privacy act requests be in writing and provide a detailed description of the records sought and/or action requested (e.g., amend, correct, or account for disclosures). Requests submitted by mail or fax shall bear the signature of the requester. Requests shall contain:

- Requester's name
- File number the Veteran
- Description of records requested
- Delivery means/mailing address
- Fees amount (if applicable)
- Does the request qualify for expedited processing?
- requester's signature

Tracking Requests. All incoming requests must be entered on a Privacy Act request log created by the Regional Office (i.e. Excel spreadsheet).

Analyzing Requests. Privacy Officers must determine whether to grant a Right of Access request by first verifying the identity of the individuals who request information.

Proof of Identity. The letter should specify if the request comes from the Veteran directly or his/her authorized representative. When a Veteran requests information from his/her VBA records, proof of identity can be established by matching the claim file number, signature, and address on the Veteran's request with the information contained within VBA's system of record.

- **By Email.**
    1. Privacy Act requests accepted via email are those received directly from the Regional Contact Centers (RCCs) where identification protocols were followed to verify the identity of the requester. In the absence of proof from RCCs that identification protocols were used, the Privacy Officer should contact the requester to obtain a signed request.
    2. E-mail requests received from the Veteran or third parties are sent to VBA FOIA corporate mailboxes such as: FOIA.VBACO@va.gov and VACOFOIASE@va.gov. These emails are then forwarded out to VBA Privacy Officers for response.
- **Third-Party.** If the request comes from an attorney, or other representative acting on behalf of the record subject, a consent form, such as VA Form 3288, *Request for and Consent to Release of Information from Individual's Records* must be provided. The consent form must be signed by record subject. Requests from authorized third parties, must supply proof of the

relationship, such as death certificates or legal guardianship form.

1. **Veterans Service Organizations (VSO).** There are no special requirements when replying to a VSO beyond the usual third-party requirements. If the VSO does not have an appropriate power of attorney, disclosure may be made only pursuant to the Veteran's written authorization.
2. **Congressional Requests.** There are generally three types of requests for information from Congress. These requests are routed through the appropriate RO Congressional Liaison Office. VA is legally permitted to disclose information about an individual without his or her consent in response to Congressional requests as follows.
    - Constituent service request – an inquiry from a member of Congress on behalf of a constituent.
        - VA may disclose information to a member of Congress or staffer in response to an inquiry made pursuant to a constituent request. The applicable routine use in VA Privacy Act systems of records permits disclosure "in response to an inquiry from the congressional office made at the request of that individual."
    - **Oversight Requests.** A request for information from a Congressional committee or subcommittee in its oversight capacity.
        - VA may disclose information in response to an oversight request that:
        - Is signed by the Chair of the committee or subcommittee; and
        - Pertains to a matter within its oversight jurisdiction.
        - These requests do not require written consent from the subject of the request. Communications from the committee ranking minority member, other members of Congress, or staff members do not qualify as oversight requests but are acceptable for the purpose of clarifying an original oversight request as long as the subsequent communications does not expand the scope of the original request. VA may provide the information sought to another member or a staffer, if specifically requested to do so by the Chair.
        - Other request – any other request for information from a member of Congress.
        - Any request for information from a member of Congress that does not fall under the two categories above should be processed under the FOIA. These FOIA requests would

Back to top

bear the member of Congress' or staffer's signature and would be opened under the member of Congress' staff member's name. For assistance, see the VA FOIA Service or the FOIA Office of the VA component that maintains the records sought.

*** CSD Exclusion List pending update

Processing FOIA/PA request:

1. Upon receipt of a FOIA or PA request in the Regional Office (RO):
    a. Claims Assistant (CA)/Veterans Service Representative (VSR)/Privacy Officer and Legal Administrative Specialists will establish EP 510. This EP shall be continued until the FOIA or PA request is completed.
    b. Enter information into Access Database tracking system. The use of the Access Database allows VA to fulfill the requirements of the "Open Government Act," which is to:
        i. Assign FOIA tracking numbers in FOIAXpress, if you are withholding or redacting information.
        ii. Track FOIA requests and provide requesters with the status of the request.
        iii. Enter the final disposition for each FOIA request.
        iv. Generate the agency's annual FOIA report.

2. If actions below cannot be accomplished **within 10 calendar days** from date of receipt of PA or FOIA request as defined in table below, Privacy Officer must prepare and send out interim response letter in letter creator (per M27-1.I.7.1.d). m27-1-pi-ch5-8-01-2022.pdf (va.gov)

3. Within 20 days of date of claim and upon completion of the FOIA or PA request, and prior to clearing the EP associated with the request, Privacy Officer will update the Access Database to reflect that the request has been closed and identify what documents were sent to the requestor.

Reference:

- VA handbook 6300.4 Procedures for Processing request for records subjected to the Privacy Act.
- VA Directive 6213 Freedom of Information ACT (FOIA).

PERSON ACTING FOR AN INDIVIDUAL

Only the individual by whose name the records are retrieved has the rights under the PA, and only that person may exercise those rights except under the following

circumstances:

1. The **Parent** of a **Minor** may exercise the child's PA rights on behalf of the child.

2. A **Court-Appointed Guardian** of an individual declared to be incompetent due to physical or mental incapacity or age may exercise that the individual's PA rights.

3. **Power of Attorney**- A person holding a properly executed and timely power of attorney form for a competent individual may exercise the PA rights of the individual within the grant of the authority contained in the power of the attorney. VBA form 21-22 Appointment of Veterans Service Organization as Claimant's Representative authorizes a service organization representative to have access to a Veteran's claims records.

Note: A VA federal fiduciary who is not a court-appointed guardian is not empowered to exercise the Privacy Act rights of the individual.

Rights an individual may have under the PA are:

- The right of access to
- Amendment of records about that individual
- Right to sue the agency for violating the PA, including VA's unauthorized disclosure of the records.

DISCLOSURE

A disclosure occurs when VA communicates VA records orally, written or electronically, to any individual, internal or external to the agency, who has little to no knowledge of the information contained in the record. Disclosure violates the PA unless there is a prior written consent from the individual whose name is on the record retrieved, or unless disclosure without written consent is authorized by the PA.

Note: If the PA authorizes disclosure, you may not disclose records if another confidentiality statute also protects those records unless authorized to do so by the statute. 38 U. S. C. § 5701, which protects benefits records (including medical care and treatment records), and 38 U.S.C § 7332, which protects records pertaining to drug abuse, alcoholism, human immunodeficiency virus (HIV/AIDs), or sickle cell anemia treatment, are examples of such confidentiality statutes.
Prior Written Consent by the individual must be addressed to VA, and must describe the records to be released, to whom, and for what purpose.

DISCLOSURE WITHOUT PRIOR WRITTEN CONSENT

Employee need to know – A VA employee who requires access to the record to perform assigned agency duties may see that record.

Freedom Of Information Act (FOIA) – The records must be disclosed when requested under FOIA, if there is no FOIA authority to withhold the records. Where a FOIA exemption permits withholding the records, the VA cannot release the records in response to the FOIA request.

Routine use – VA may release records pursuant to a published routine use in the system of records which covers those records, for a purpose compatible with the reason for gathering the records.

Requests from Law Enforcement Entities – VA may release PA records to state or Federal law enforcement authorities engaged in investigations when they request the records if the request is written; and is signed by the ***head of the requesting law enforcement entity***, or ***by a designee***; is for an authorized civil or criminal law enforcement purpose; is specific as to the record or portion of the records sought; and is specific as to the particular law enforcement investigating activity for which the record is sought.

Court Order – VA may disclose non 38 U.S.C 7332 protected records in response to a court order to do so. A court order is a command that VA release the records to a specified individual or entity by member of the judicial branch who has the authority to punish the refusal to produce the records by holding VA or a VA employee in contempt of court. A subpoena almost always is not a court order, and an administrative order from a state or Federal executive branch component is not a court order. Records protected by 38 U.S.C. 7332 may be disclosed if authorized by an appropriate order of a court of competent jurisdiction (Federal, State or local) under the provisions of 38 C.F.R. § 1.490.

Note: If a PO receives a court order, he or she is required to send a copy of the court order to their local OGC, for guidance.

AMENDMENT OF RECORD

An individual has the right to see VA records about themselves which are retrieved by their name or other identifiers, and the right to have the VA amend those records when the records are not **accurate**, **timely**, **complete**, and **relevant.**

Procedures For Handling Requests for Access To Or Amendment Of Records

1. This paragraph establishes procedures whereby an individual may:
   a. Request notification of whether VA maintains or has disclosed, a record pertaining to him or her which is maintained in any system of records.
   b. Request a copy of, or other access to such record, or obtain an accounting of its disclosure.

c. Request that the record be amended; and

d. Appeal the initial adverse determination of any such request.

2. The procedures specified in this paragraph apply only for records retrieved by personal identifier from the following systems of records:

a. The systems of records for which a System of Records Notice (SORN) has been published by VA in the Federal Register pursuant to section 552a(e)(4) of the Privacy Act.

b. Those records contained in Government-wide personnel system of records for which a SORN has been published in the Federal Register by another agency such as the Office of Personnel Management (OPM) (SORNs published by those agencies govern notification, access, and amendment of such records even though they are maintained by VA); or

c. Those records contained in a system of records operated by or on behalf of VA by a government contractor to accomplish a VA function. For this purpose, any such contractor and any employee of such contractor is considered to be an employee of VA and subject to the criminal penalties contained in 5 U.S.C. 552a(i).

PRIVACY ACT EXEMPTIONS

The Privacy Act of 1974, as amended, prohibits agencies from disclosing information about an individual without the individual's written consent, unless the disclosure is pursuant to one of the 12 statutory exceptions. The 12 exceptions contained at 5 U.S.C. § 552(b) allow disclosure as follows:

1. To those officers and employees of the agency which maintains the record, who have a need for the record in the performance of their duties.
2. When disclosure is made under the FOIA.
3. For an established routine use identified in the SORN that has been published in the Federal Register.
4. To the Census Bureau for purpose of planning or carrying out a census or survey.
5. To a recipient who has provided the agency with adequate written assurance that the record will be used solely for statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable.
6. To the National Archives and Records Administration (NARA) for historical preservation if the Archivist determines the record has historical value.
7. To another agency or to an instrumentality of any governmental jurisdiction,

Back to top

within or under the control of the U.S. for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.

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 such individual.
9. To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee.
10. To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accountability Office.
11. Pursuant to the order of a court of competent jurisdiction.
12. To a consumer reporting agency in accordance with the Debt Collection Act.

PROCESSING COURT ORDERS

VA may disclose records in response to a court order. A court order is a written directive or mandate, signed by a court or judge, directing that some action be taken or prohibit an action be taken. Subpoenas are not court orders unless signed by a judge or some other official who has the inherent power to enforce the order.

Note: If a PO receives a court order, he or she is required to send a copy of the court order to their local OGC, for guidance before they respond to the Court order.

In order to process court order request, the “court” must be a part of the judicial branch of government, not part of either the executive or legislative branches. An “order” must be a document signed by a court official with the power to enforce the order, contempt sanctions. If the court official must go to some other entity to enforce the order, e.g., to a federal district court judge, the order does not qualify as a court order for purposes of the PA. An order signed by an administrative law judge, or a state board would not qualify as a court order.

The order must specifically require VA to produce the records. An order giving VA permission to file records if it chooses to do so will not qualify as a court order for this exception.

VA treats order of both federal and state courts as qualifying court order for the purposes of subsection (b)(11) of the PA.

The PA cannot be used to defeat a normal court proceeding. Rather, VA must

Back to top

comply with the court and with the PA. For example, when VA produces records pursuant to a court order, VA must mail a notice of the disclosure to the last known address of the subject of the records. If the subject of the records is present in the court when the records are produced, this requirement is satisfied.

The person seeking the court order is not required to show a need for the records, only that they are relevant to the proceedings under Federal Rule of Civil Procedure 26 (b) (11).

The Privacy Act of 1974, as amended, prohibits agencies from disclosing information about an individual without the individual's written consent, unless the disclosure is pursuant to one of the 12 statutory exceptions. The 12 exceptions contained at 5 U.S.C. § 552(b) allow disclosure as follows:

PRIVACY EVENT TRACKING SYSTEM (PSETS)

The Privacy Security Events Tracking System (PSETs) is VA's only authorized method for tracking and reporting privacy complaints and incidents.

In August 2023, DBRS migrated PSETs to a ServiceNow platform.

Note: PSETS in ServiceNow is supported by Chrome and Edge.

Access to the system is role based and uses an active directory for authentication.

When using the system please utilize the DBRS PSETs in ServiceNow Guides and Resources located on the DBRS Primary Site - Home (sharepoint.com).

Legacy PSETS Events

As a reminder, the last seven (7) years of data has been transferred to the new platform in accordance with the records control schedules applicable to PSETS. Legacy events have all been worked and are in various states (e.g., remediation, final review, or closure). Please make sure you're keeping up with your tasks (found on the Privacy Event Dashboard Tasks tab). It's important to note that some legacy events need manual massaging to progress in state all the way to closure. If you have an issue with a legacy event, please send an email to the VA DBRS Mailbox (vadbrsmailbox@va.gov) and the DBRS staff will help move it along for you.

Breach Notification Letter Inputs

The new process for entering your letter inputs directly into PSETS is an important process for ensuring letter quality before letters make their way to our Veterans. The DBRS staff are reporting there is still some confusion with this process.

Tips for writing letters:

- Write in complete sentences
- in the second person voice
- Using proper capitalization, punctuation, and spelling.

It's imperative that you enter the right information in the fields marked for Veteran letter. It is good practice to read the letter out loud. If the letter doesn't flow or read well, DBRS staff will reject approval of the letter and provide feedback on the Activity tab.

(see DBRS SharePoint Site for additional recommendations)

Incomplete/Missing Required Information

While use of the templates lessens the time it takes to input an event, you're still required to ensure the information you're submitting is both accurate and complete. DBRS staff are reporting incomplete and missing required information for incidents which requires them to reach out to you for corrections. Please ensure you complete all the fields in Information at Risk and Info Storage/Equipment at Risk. This means that you should enter the quantity and all other fields on each row. Also, it's important that if you use a template that has several data options, that you remove those that do not apply by clicking the x. We encourage you to review and follow the PSETS in ServiceNow User Guide to ensure you're doing this correctly.

PSETS – COMPLAINT & INCIDENT REPORTING

Distinguishing between a Complaint versus Incident versus Data Breach/Violation

A **complaint** is when a Privacy Officer receives information from an individual regarding an alleged violation of the individual's privacy. It may include issues related to impermissible access or disclosure of information covered under any of the privacy and confidentiality laws and regulations pertaining to VA. Access and amendment complaints, which pertain to denial of access and amendment rights, are considered complaints. Complaints are required to be entered into PSETS.

Example: A Veteran submits an alleged complaint with the PO stating that a VR&E counselor impermissibly accessed his health record. After investigation it was determined that the VR&E counselor accessed the Veteran's health record in order to provide information relative to placement of the Veteran within the VR&E program. The VR&E counselor accessed the health record in the performance of her official duties.

An **incident** occurs when it is confirmed that a violation of privacy practices/policy has occurred that has resulted in access, loss, or disclosure of sensitive information outside VA or not in compliance with VA practices/policy. An incident becomes a **breach** only upon determination by the Data Breach Core Team (DBCT) who does a risk assessment to determine if the incident constitutes a reportable breach.

For example, C&P exams faxed to the incorrect location, employee accesses PII of co-

worker out of curiosity or service treatment records mailed to the incorrect Veteran.

VA Incident Resolution Service and Data Breach Core Team (DBCT)
(Refer to VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information)

VA Publications

The DBCT provides administrative oversight of incident reporting involving the loss or compromise of data and has the authority and responsibility to escalate any incident, regardless of the risk assessment. DBCT works with the Incident Resolution Service in responding to breaches and addressing notification requirements from a collaborative perspective. DBCT determines the need for initial notification and credit protection offers to individuals whose sensitive personal information was involved in a breach. DBCT coordinates response actions until the incident is resolved.

The VA Incident Resolution Service serves as liaison between the functional area(s) affected in a privacy/security incident, VA organizations, and certain non-VA entities such as the Office of Management and Budget (OMB), the Government Accountability Office (GAO), and Congress. The VA Incident Resolution Service implements and follows up on decisions made by the DBCT. The VA Incident Resolution Service is responsible for drafting quarterly and ad hoc reports to Congress.

Processing a Complaint and/or Incident

A privacy complaint occurs when an individual lodges a complaint, oral or in writing, about a privacy practice, violation, or breach to a PO. A complaint can be lodged by a Veteran, Veteran's family, employee, or any member of the public. A complaint must be completed **within 60 days**, from the date the complaint was received.

A complaint or incident must be documented into PSET **within one (1) hour** of initial notification. The PO can discuss the complaint with VA employees who are assisting with the investigation or who are being investigated. *Please stress the confidentiality of all statements given during the investigation of a potential privacy violation or breach.*

The PO should create a new administrative file folder to track the complaint/incident and information related to the PSET. The administrative file folder should be saved by the PSETS ticket number.

Note: *Recommend electronic record keeping.*

It is recommended the PO contact the complainant to inquire about details regarding their side of the story. All information should be documented. It is recommended using a Report of Contact form (VA Form 27-0820 Report of General Information). Please note, at this stage the questioning should be limited to fact finding only.

The Privacy Officer can discuss the complaint with VBA employees who are assisting

with the investigation or who are being investigated. This may include supervisors, other employees, Veterans; and anyone who will assist you in thoroughly investigating the complaint.

To perform the fact finding, the PO must provide the right to Union representation to any bargaining unit employee they interview. You may want to consult with the local Human Resource office for the process of notifying the employee of the fact-finding interview. The objective of the fact finding is to try to determine if the employee's actions were appropriate and in accordance with VA privacy policy. Once all the information surrounding the complaint is collected, the PO must decide whether or not the privacy complaint is valid.

The validity of a complaint is determined by whether or not an inappropriate behavior or action occurred in violation of VA privacy policy and practices. Regardless of the validity of the complaint or the action taken, the PO should always respond to the complainant in writing.

The complainant should only be provided with general information, not specific details regarding any mitigation or corrective action(s) taken. However, sufficient details should be noted in the letter which explains, especially when dealing with an access complaint based on a SPAR, why this VA employee had access due to his specific job duty or why your investigation determined that the complaint was unfounded. The complainant may not receive disciplinary action taken against a VA employee; only the appropriate mitigation act that has taken place.

PRIVACY THRESHOLD ANALYSIS (PTA) AND PRIVACY IMPACT ASSESSMENT (PIA)

Congress passed the Electronic Government Act of 2002 to encourage the use of electronic government by the public. The Act recognized the fact that technological changes in computers, digitized networks, internet access, and the creation of new information products have made information much more available. The Act also recognized that these advances have important ramifications for the protection of personal information contained in government records and systems. Section 208 of the Act requires federal agencies to conduct a PIA on information technology systems that collect, maintain, and/or disseminate "personally identifiable information".

As prescribed in VA Directive 6502, Enterprise-wide Privacy Program, VA officials responsible for the initiation and implementation of rulemaking, IT systems, and/or projects are required to complete a PTA annually. If a PTA determination indicates no PIA is required, the PTA will be included in the Authorization and Accreditation (A&A) documentation as official record that no PIA is required. (A PIA is required for all systems that are subject to the A&A process; these provisions are codified in OMB Circular A- 130, Appendix III)

**PTAs and PIAs are reviewed by VBA Central Office Privacy Officers. As of January 1,*

2020, reviewing of PTAs/PIAs for VBA Regional Offices are covered by Area Boundaries. Reference (Area Boundaries fact sheet)
https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=1050&FType=2

A PTA will be conducted when any of the following are applicable:

- Develops or procures any new technologies or IT systems that collect, maintain, or disseminate PII and/PHI.
  - Systems for which a PTA has not been officially verified by the Associate Deputy Assistant Secretary for Policy, Privacy, and Incident Response or their designee will not be considered certified and cannot be accredited.
  - Unaccredited systems will not be granted an Authorization to Operate (ATO).
- Initiates a new collection of PII and/or PHI on ten (10) or more persons is proposed.
- Revises existing systems. If the project, rulemaking, and/or IT system, are not covered under a current SORN, a new or updated SORN may be required.
- Issues a new or updated rulemaking that affects PII and/or PHI. If an agency rulemaking results in or is likely to result in a new collection or use of VA maintained PII and/or PHI.
- All Project Management Accountability System (PMAS) programs or projects.
- If a project, rulemaking, and/or IT system have statutory authority to collect or use PII/and or PHI.
- A PTA must be completed for every new electronic data collection or when a major change occurs to an existing IT system.

Annually, the System Owner is required to reassess and certify that no major changes have occurred by completing the PTA. Completed PTAs should be submitted to the VA Privacy Service annually according to their annual scheduled due date. In the event of a major change or an expired PIA, a new PIA will be required.

PTA/PIA's:

Standard PTA Template: This template is required for efforts associated with the Federal Information Security Management Act (FISMA) and (A&A) processes or when it has been determined that you need to complete a PTA outside of the PMAS process.

1. The System Owner is responsible for completing the Standard PTA and coordinating with other relevant stakeholders such as the Privacy Officer.

2. VA Privacy Service is responsible for the review and determination of

standard. PTA's and IPT Privacy Officers are responsible for the review and determination of PMAS PTA's.

**NOTE: VA Privacy Service is responsible for the review and determination of Standard PTA's and IPT Privacy Officers are responsible for the review and determination of PMAS PTA's.*

The PIA determines whether an existing SORN should be revised or if a new SORN is required.

VA Administrations and Program Offices are required to complete a PIA for all new and substantially changed Information Technology IT systems, rulemakings, programs, and/or projects that have been determined by the adjudication of the PTA to collect, maintain, or disseminate PII and/or PHI. If there have been no major changes made to the system, then a PIA is required every three years.

A PIA is required when the PTA identifies that PII and/or PHI is being collected, maintained, or disseminated. As set forth in the VA A&A process, systems will be assessed to identify whether PII and/or PHI is being collected or changes have occurred that require a new PIA.

There are PTA and PIA training slides that provide an overview of the process, define the roles and responsibilities of key staff when completing the PTA and PIA as well as a detailed demonstration of what is required in each section of the templates.

Additional Helpful Information on PIAs

Important Links

- VA Directive 6508, Privacy Impact Assessments
- VA Publications
- PIA and PTA templates along with PIA and PTA Training are available at http://vaww.oprm.va.gov/privacy/pia.aspx
- PIA Training Supplemental
- All published VA PIA's

Contact Information

For more information about Privacy Impact Assessments, please visit the PIA website http://vaww.privacy.va.gov/PIA.asp or email the VA Privacy Service who handles PIA assessments at PIASupport@va.gov**.**

For more information about PIAs, contact the VA Privacy Service at 202.273.5070 or privacyservice@va.gov

SYSTEM OF RECORDS NOTICE (SORN)

The Privacy Act of 1974 requires all federal agency's SORN to provide public notice regarding the establishment or modification of a system of records. SORNs explain how the information in the records is used, retained, and may be accessed or corrected, and whether certain portions of the system are subject to PA exemptions for law enforcement, national security, or other reasons.

VBA Central Office Privacy Officers work with ISSOs, system owners and others deemed necessary, to create, review, and/or update VBA SORN.

A SORN is the notice published by an agency in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system.

A SORN identifies the following:

- system of records
- purpose(s) of the system
- authority for maintenance of the records
- categories of records maintained in the system
- categories of individuals about whom records are maintained
- routine uses to which the records are subject
- additional details about the system

A SORN is required when ALL of the following apply:

- Records are maintained by a Federal agency, and
- The records contain information about an individual, and
- The records are retrieved by name or unique personal identifier

A SORN includes the routine uses to which the records are subject. Routine uses apply to information sharing external to VA. The term "routine use" is defined, with respect to the disclosure of a record, as the use of such record for a purpose which is compatible with the purpose for which the record was collected. The routine use provision of the PA functions as one of the exceptions to the statute's general prohibition against the disclosure of a record without the written consent of the individual to whom the record pertains. VA may only establish routine uses for a system by explicitly publishing the routine uses in the relevant SORN.

NOTE: A system of records (SOR) is any group of records under the control of an agency about an individual, from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying information assigned to the individual.

A record in a system of records must contain two elements: a name or unique personal identifier and at least one item of personal information.

Back to top

If a retrieval of personal information is possible, but not actually done, or if it depends on memory or a sequential search, the collection of records is not a system of records. However, creating a retrieval method or cross-index arranged by personal identifier for randomly filed records makes that record collection a system subject to the provisions of the Act.

More information regarding SORNs and SORs can be found at the below link:

System of Records Notice (sharepoint.com)

PRIVACY WALK THROUGHS

VA Directive 6509, requires Privacy Officers to conduct walkthroughs of all assigned offices to ensure security and privacy-related activities are being followed and provide guidance, as needed, to employees on proper procedures for the handling of sensitive personal information.

It is important for the Privacy Officer to interact with staff while on rounds. This allows for staff to become familiar with the Privacy Officer and helps to provide privacy awareness throughout the Office.

Examples of questions Privacy Officers can ask of staff are:

1. Do you know who the Privacy Officer is, and do you know how to reach them?
2. Who is responsible for release Veterans information?
3. What do you do if you witness a privacy incident?
4. Do you know who is responsible for processing amendment record request?
5. Do you have any logbooks in your area?
6. Does your fax cover sheet contain the confidentiality clause?
7. Is there a shred-bin or locked container in your area?
8. Are your printers, copiers, and fax machines publicly accessible?
9. What is your process for securing documents containing PII?

The Privacy Officer must identify any privacy issues such as visible PII on computer monitors in high traffic areas, audible PII in phone conversations, PII on sign-in sheets, unattended documents containing PII. The intent of the Privacy Walk-Through is to identify privacy issues, communicate with staff and management when vulnerabilities are identified, and correct any issues immediately. Documenting the findings could be useful in identifying any reoccurring issues which might require a more in-depth evaluation.

References:
VBA Directive 6509

PRIVACY OFFICER REVIEW OF CONTRACTS

The Privacy Officer (PO) is responsible for reviewing the Statement of Work (SOW) or Performance Work Statement (PWS) and the VA Handbook 6500.6, Appendix A checklist, to determine if VA sensitive information will be included in the contract.

The PO must work collaboratively with the Information System Security Officer (ISSO) and the Contracting Officer (COTR/COR) to ensure the checklist is completed accurately and in a timely manner.

The purpose of the VA Handbook 6500.5 is to establish the security and privacy procedures, responsibilities, and departmental framework for incorporating security and privacy in the system development life cycle (SDLC) of IT assets that store, process, or transmit VA information by, or on behalf of, VA as required by the E-Government Act of 2002, Public Law 107-347; to include *Title III, The Federal Information Security Management Act (FISMA)*, and VA Directive and Handbook 6500, *Information Security Program*.

This handbook is dependent upon the security requirements established in VA Handbook 6500 and other handbooks in the 6500.x series. (see Reference section for a list)

The Privacy Officer should always utilize VA Handbook 6500.6 Appendix A Crosswalk as a guide, when reviewing VA Handbook 6500. 6 Appendix A, Checklist.

Contract Review References:

- VA Handbook 6500.5 Incorporating Security and Privacy Into The System Development Life Cycle
- VA Handbook 6500 Information Security Program
- VA Handbook 6500.6, Contract Security
- VA Handbook 6500.6, Contract Security, APPENDIX C, Reference
- VA Handbook 6500.6, Contract Security, APPENDIX D, Minimum Security Controls for VA Information Systems
- VA Handbook 6500.6, Contract Security APPENDIX E, VA Control Configuration Standard
- VA Handbook 6500.6, Contract Security APPENDIX F, VA Password Management
- VA Handbook 6500.6, Contract Security APPENDIX G, National Rules of Behavior

REVIEWING PRESENTATIONS DISPLAYING PERSONALLY IDENTIFIABLE INFORMATION (PII)

According to VA Directive 6511, Presentations Displaying Personally Identifiable Information, the Privacy Officer will review the presentation for PII, and information

exempt from release under FOIA. If no PII or information exempt from release under FOIA is used in the presentation, the Privacy Officer will approve the presentation. If PII or information exempt from release under FOIA is present, the Privacy Officer will disapprove the presentation unless there is an applicable signed, written authorization from the subject of the information. If the Privacy Officer approves the presentation, he or she must sign the Presenter Certification (VA Form 0897) and provide the form and approved presentation to the presenter. The presenter will provide the form and approved presentation to the event organizer.

1. REASON FOR ISSUE: This Directive establishes the policy that personally identifiable information (PII) and information that is not releasable under the FOIA, as amended, must not be included in presentations that may be seen by non-VA parties, a term which includes members of the public, and VA employees, volunteers, trainees, contractors, or other appointees without an official need to know such information. The document addresses methods of sanitizing presentations that may be made available to these individuals or groups. The requirements set forth in this Directive ensure that these presentations and materials do not contain PII, or information exempt from release under FOIA. It also implements the policies pertaining to privacy reviews, as discussed in VA Directive 6502, Privacy Program.

2. SUMMARY OF CONTENTS: This Directive describes the responsibilities, requirements, and procedures for eliminating PII or information exempt from release under FOIA from presentations that may be seen by non-VA parties. This Directive includes guidance for conducting privacy reviews of presentations, and the criteria for when presenters must self-certify that their presentations are devoid of PII, or information exempt from release under FOIA.

3. RESPONSIBLE OFFICE(S): Office of the Assistant Secretary for Information and Technology (005), Office of Information Security (005R), Office of Privacy and Records Management (005R1), VA Privacy Service (005R1A).

4. RELATED DIRECTIVES: VA Directive 6502, VA Enterprise Privacy Program, VA Directive 6511, Presentations Displaying Personally Identifiable Information. VA Publications

MAILING OF SENSITIVE PERSONAL INFORMATION (SPI)

Mail containing information under VA control must be shipped via the most secure, economical, and effective means practicable. VA requires the protection of Sensitive Personal Information (SPI) during the mailing process. As such, special procedures must be used for its protection. Mail, including both hardcopy and electronic media, that is lost, sent to the wrong recipient, or stolen can result in identity theft. Identity theft may result in personal hardship to individuals, including Veterans, dependents, and VA

personnel. In order to ensure the adequate protection of mailing both within and from VA.

Any person sending or redirecting mail must ensure that it is secured before placing it into the mail system.

Envelopes, parcels, packaging, or boxes containing SPI must be secured in a manner that prevents unauthorized access, tampering, or accidental loss of contents.

Window envelopes must show the recipients' name and address, but no other information. Social security numbers, claim file numbers, dates of birth or other SPI, must not be viewable through a window envelope.

Mailing labels must only display the amount of personal information necessary for the mail to reach the addressee.

If a facility uses mass production letters with mail merge and the letters are run through a machine, the letters containing SPI must be sealed prior to delivering them to the United States Postal Service (USPS) or other shipping service, such as United Parcel Service (UPS) or Federal Express (FedEx).

Use of Secure Delivery and Package Tracking: Original documents, as defined in Paragraph 5b of this policy, must be sent via a secure delivery service that tracks mail from pick-up to delivery. Examples of services that provide this type of online tracking system are FedEx Insight, UPS Ground, and USPS Priority Mail Veterans' documents may be sent via untracked mail only if they are copies, not originals, due to the possibility of loss or misplacement.

Outgoing mail that contains SPI and is sent to Veterans, dependents, business partners (e.g., VSOs and health insurance plans) or other members of the public will be shipped using the USPS unless the package contains original documents or VA agrees to a request from the Veteran, beneficiary, business partner, or other member of the public to use a tracked delivery service.

In accordance with 38 C.F.R. § 1.526(j), a copy of the VA record requested to be transmitted by certified or registered mail, airmail, or special delivery mail will result in the postal fees being added to the other fees charged for providing such copies. However, if the originating office determines that the sensitivity of the mail demands it, the office may use a tracked delivery service for the mailing of copies. The originating office will bear the additional cost of using this shipping method.

VA Directive 6609: Every individual article or grouping of mail, however sent, that contains SPI that is sent from VA to any VA personnel must be accompanied by a notice sheet (appendix A) containing language that explains that there are penalties for violations of the PA and the HIPAA Privacy Rule. These notice sheets must be inserted as coversheets to the document.

A notice sheet does not need to be used when sending mail if the information is being mailed to the individual to whom the information pertains or there is a signed authorization from the individual to whom the information pertains for the release of the information to the recipient.

Any disclosure of information protected by 38 U.S.C. § 7332 pursuant to the individual's written consent must be accompanied by the following statement, in accordance with 38 C.F.R. § 1.476:

"This information has been disclosed to you from records protected by Federal confidentiality rules (38 CFR Part 1). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 38 CFR Part 1. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient or patient with sickle cell anemia or HIV infection."

The notice sheet must also be inserted into internal/interoffice mail envelopes (e.g., Optional Form 65Cs or "holey joes") that contain documents containing SPI.

Notification with Untracked Mail: If a tracking service is not used for bulk mailings containing non-original documents with SPI sent within and between VA entities (e.g., from a VA entity to a business partner or vice versa), the originating office must alert the receiving office that a package with SPI is on its way and the receiving office must inform the sending office of the package's arrival.

Internal Special Attention Mail: For all bulk mailings internal to VA that contain original documents with SPI (e.g., claim files), a stamp or label denoting that special attention is needed must be used. These stamps or labels must be placed inside the larger package but on the outside of any internal package, envelope, or groupings of documents. This is done in order to facilitate delivery to the correct recipient. All stamps or labels must provide space for the name of the sender and his or her routing symbol, and the recipient's name and routing symbol (see Appendix B, Special Attention Mail). The sender must fill-in the information on the attention stamp or label. The sending office is responsible for the cost and for providing all special attention stamps or labels.

Mail Containing Electronic Media: Electronic media (e.g., CDs) that contains SPI must be encrypted and password protected in accordance with the current requirements of VA Handbook 6500, Information Security Program, with respect to storage of VA information on portable storage devices and shipped via a secure delivery service that tracks the mail from pick-up to delivery.

Exceptions: Encryption is not required to mail electronic media (e.g. CD or DVD) for the following:

1. Mailing records containing the SPI of a single individual to:

   - That person (e.g. the Veteran's, beneficiary's, dependent's, or employee's own information) or to that person's legal representative (e.g., guardian, attorney-in-fact, attorney, or VSO). Such information may be mailed to an entity, not otherwise the subject of an exception, with the express written waiver of the individual. Such information may be mailed via USPS regular mail unless tracked delivery service is requested and paid for by the recipient.

   - A business partner such as a health plan or insurance company, pursuant to a documented risk assessment. The risk assessment should be performed in consultation with the appropriate Information Security Officer (ISO).

   - A court, adjudicative body, parties in litigation, or to persons or entities in the course of a judicial or administrative proceeding.

   - Congress, law enforcement agencies, and other governmental entities.

   - Mailing of electronic records containing SPI to a person or entity that does not have capability to decrypt it:

     - Such media must be password-protected, and the password must be transmitted separately from the electronic media containing the SPI (e.g., by telephone, email, or separate mailing). These media must be shipped via a secure delivery service that tracks the mail from pick-up to delivery. If these items are shipped in bulk, the delivery service must use the equivalent of a hard cover, locking container. This locking container service is available from certain shipping companies.
     -

RECORDS MANAGEMENT

The Records Section facilitates VBA's mission to carry out records management in an efficient and effective manner. Policy and direction are given for records during their life cycle: creation, maintenance/use, and disposition.
Records are the foundation of open government, supporting the principles of transparency, participation, and collaboration. Well-managed records can be used to assess the impact of programs, to improve business processes, and to share knowledge across the government. Records protect the rights and interests of people and hold officials accountable for their actions.

POs have a duty to update and accurately maintain a portion of their station's file plan. The below link will provide guidance on records management.

https://dvagov.sharepoint.com/sites/VACOVBAOA/Records/SitePages/Home.aspx

VBA Directive 6300; Records and Information Management: VA Publications

PRIVACY PROGRAMS

VA Privacy Programs:

- **VA Privacy Service**
  VA Privacy Service is VA's key policy advisor on implementing laws and providing privacy guidance, including the Privacy Act of 1974 (5 U.S.C. § 552a) and privacy provisions of the Federal Information Security Modernization Act (FISMA) of 2014, and of the E-Government Act of 2002. VA Privacy Service provides consultancy services to VA20 and carries out its role as privacy consultants through operational areas: Privacy Risk Management Compliance, Incident Management and Response, Privacy Consultancy, Communication, Training and Outreach, and Privacy Policy Development & Implementation. VA Privacy Service collaborates with Other Key Officials and POs in VHA, VBA, NCA, Administrations, and Program Offices to implement privacy policy.

Additional information regarding VA Privacy Service can be found at the below link:
VA Privacy Service Privacy Hub - Home (sharepoint.com)

STANDARD OPERATING PROCEDURES (SOP)

The PO should develop the following SOPs:

- How their station process Privacy and FOIA request
- How their station process privacy violation and complaints.
- How their station process amended records request.
- How their Public Contact staff process Privacy Act/FOIA request at their stations.
- A SOP outlining their privacy programs. (See VA Directive 6509)
- A SOP outlining the process for reviewing training material for PII.

VBA PRIVACY SHAREPOINT SITE

To enroll in the Privacy Officer Mail group, send an email to: VAVBAWAS/CO/Privacy Privacy.Vbavaco@va.gov

Send updated PO information to the privacy mailbox. The Privacy Officer information will be included on the Privacy Officer List - PowerApps with your information. It is important that you verify that your information is current and accurate.

VBA Privacy Officers - Please use this group when you want to query the large group of privacy officers with questions: such as facility-specific policy development, performance standards, best practices, training, or general news. Sharing information

that is pertinent to other PRIVACY OFFICERs is highly encouraged.

https://dvagov.sharepoint.com/sites/VACOVBAOA/Privacy/SitePages/Home.aspx

PROFESSIONAL MEMBERSHIP ASSOCIATION

Founded in 2000, the International Association of Privacy Professionals (IAPP) is the world's largest association of privacy professionals with more than 7,000 members in 52 countries. The IAPP helps define, support, and improve the privacy profession through networking, education, and certification.

Hear what the experts are saying about the latest privacy trends and issues. IAPP events and programs are an invaluable forum for engaging with peers and mentors, advancing your skill levels, and gaining insight into the latest issues from the perspective of internationally recognized experts and industry leaders on privacy, security, and information sharing.

Privacy Certification - In the rapidly evolving field of privacy and data protection, certification demonstrates a comprehensive knowledge of privacy principles and practices and is a must for professionals entering and practicing in the field of privacy. Achieving an IAPP credential validates your expertise and distinguishes you from others in the field.

To learn more about IAPP, register, locate educational materials for review, or to check out the below credentialing programs, you may visit their website at: International Association of Privacy Professionals (iapp.org)

PRIVACY CERTIFICATIONS

The Certified Information Privacy Professional/Government (CIPP/US) is the publicly-available privacy certification designed for employees of U.S. federal government agencies as well as U.S. state, county, and local governments. It also is available to vendors, suppliers, and consultants who serve government clients.

The CIPP/G addresses U.S. government privacy laws, regulations, and policies: those specific to government practice as well as those more broadly applicable to both the public and private sectors in the United States. The program also covers U.S. government-standard practices for privacy program development and management, privacy compliance and auditing, records management and agency reporting obligations for privacy.

The IAPP created the CIPP/G program with the assistance of privacy officers from U.S. federal agencies that include the USPS, the Department of Justice, the VA, OMB and the Internal Revenue Service, as well as U.S. state agencies.

If you obtain certification through IAPP, please contact the VA Privacy Service to include your name on their list of VA employees. VA Privacy Service has a corporate

membership and your annual association fees would then be paid by VA. Note: VA does not pay for an employee to take a certification examination. This is a personal responsibility.

PRAD – PRIVACY AND RECORDS ASSESSMENT DIRECTORATE

The PRAD is a high performing, experienced team consisting of Program Analysts and an Information Security Specialist for a total of 15 personnel. Each team member is a subject matter expert that mutually supports the other, the PRAD organization, and Compliance Risk and Remediation's overall mission requirements.

As a team, we strive to move OIT, our partners and the VA towards a better compliance posture to fully and comprehensively secure veteran's information.

PRAD uses FSAs as a means of conducting ongoing monitoring to assess Privacy and Records Management Programs for compliance with applicable policies, statutes, and regulations. These self-assessments also allow you to monitor and evaluate the performance of the specific program, identify weaknesses and areas of non-compliance and to set priorities for how you mitigate risks and improve your program over time. The FSA identifies and focuses on remediation efforts toward non- compliant areas in order to reduce risks associated with non-compliance. It also enables you to identify compliant areas, so you can celebrate successes and best-practices.

Only the Primary Privacy Officer, Records Manager or their alternates to complete the applicable FSA for their area of responsibility. This is important in that the FSA should be completed by someone with subject-matter expertise, detailed knowledge of the program and awareness of the findings of on-going monitoring activities that determine the responses within the FSA. FSAs should NOT be treated as a suspense that can be entered by anyone at the end of the quarter.

The below link will provide guidance on completing assessments, how to gain access, and FSA success tips.

Compliance, Risk, and Remediation - Home sharepoint.com)

Reference: VA Directive 6502.3.j.(1)(c)(d) and (2)(a)(b)

PRIVACY REFERENCES

PRIVACY ACT OF 1974

The Privacy Act, 5 U.S.C. 552a, implemented by 38 CFR Section 1.575-1.584. Generally, the Privacy Act provides for the confidentiality of individually identified and retrieved information about living individuals that is maintained in a Privacy Act system of records and permits disclosure of Privacy Act-protected records only when specifically authorized by the statute. The Privacy Act provides that the collection of information about individuals is limited to that which is legally authorized, relevant, and

Back to top

necessary. All information must be maintained in a manner that precludes unwarranted intrusion upon individual privacy. Information is collected directly from the subject individual to the extent possible. At the time information is collected, the individual must be informed of the authority for collecting the information, whether providing the information is mandatory or voluntary, the purposes for which the information will be used, and the consequences of not providing the information. The Privacy Act requires VA to take reasonable steps to ensure that its Privacy Act-protected records are accurate, timely, complete, and relevant. ***NOTE:*** *The information collection requirements of the Paperwork Reduction Act must be met, where applicable.*

NIST 800-53 SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS.AND ORGANIZATIONS

https://doi.org/10.6028/NIST.SP.800-53r5

PURPOSE. This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The publication also describes how to develop specialized sets of controls, or overlays, tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). Addressing both security functionality and security assurance ensures that information technology products and the information systems built from those products using sound systems and security engineering principles are sufficiently trustworthy.

6213 Freedom of Information Act (FOIA)

VA Publications

Purpose - To establish Department of Veteran Affairs (VA) policy to implement the Freedom of Information Act, 5 U.S.C. § 552 as amended; The FOIA Improvement Act of 2016; Executive Order (EO) 13392 of December 14, 2005, Improving Agency Disclosure of Information; Title 38 Code of Federal Regulations Part 1, Procedures for Disclosure of Records Under the Freedom of Information Act, 38 C.F.R. §§ 1.550-1.562; and the Presidential Memorandum of January 21, 2009: Memorandum on Transparency and Open Government.

6300.4 PROCEDURES FOR PROCESSING REQUESTS FOR RECORDS SUBJECT TO PRIVACY ACT

VA Publications

PURPOSE. This handbook sets forth procedures for processing requests for access to or amendment of records under the Privacy Act of 1974 (Privacy Act). Definitions of the terms used in the Privacy Act, a discussion of criminal penalties for violating the Privacy Act, and information concerning the application of the Privacy Act to Department of Veterans Affairs (VA) contractors are provided.

6300.6 PROCEDURES FOR RELEASING LIST OF VETERANS' & DEPENDENTS' NAME & ADDRESS

VA Publications

PURPOSE. This handbook sets forth procedures for implementing 38 U.S.C. 5701(f)(1) that authorizes the disclosure of names and/or addresses of present or former members of the Armed Forces and their dependents (beneficiaries) to certain nonprofit organizations. 38 U.S.C. 5701(f)(1) limits disclosures to Veterans' service and other nonprofit organizations to notifying Veterans of Title 38 benefits and providing assistance to Veterans in obtaining them. Benefits under Title 38 include compensation, pension, education, medical care, vocational rehabilitation, and loan guarantees. In addition, sections 6301 to 6306, authorize an outreach services program to ensure eligible Veterans are advised of benefits and services administered by VA and other governmental entities. These include programs and benefits provided by state or local entities as well as Federal programs other than those authorized by Title 38, that give assistance in applying for these benefits. Section 6304 of Title 38 establishes Veterans Assistance Offices and section 6306 requires the provision of outreach services and notification about benefits and services in cooperation with Federal, State, or local governmental institutions, or recognized national or other organizations.

6309. COLLECTION OF INFORMATION PROCEDURES

VA Publications

PURPOSE. This handbook provides guidance and outlines procedures for the management of collections of information activities. Instructions for developing a collection of information are included, as is the process for requesting Office of Management and Budget (OMB) review. It also supplements the policies and responsibilities prescribed in VA Directive 6309, Collections of Information. Together, the handbook and the directive provide the necessary information to maintain an effective program.

6500. RISK MANAGEMENT FRAMEWORK FOR VA INFORMATION SYSTEMS VA INFORMATION SECURITY PROGRAM

Back to top

VA Publications

PURPOSE. This Handbook establishes the foundation for Department of Veterans Affairs (VA) comprehensive information security and privacy program and its practices, based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*; NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*; and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, that will protect the confidentiality, integrity, and availability of information created, processed, stored, aggregated, and transmitted by VA's information systems and business processes.

1. This Handbook provides the minimum mandatory security control standards for implementation of VA Directive 6500, *Managing Information Security Risk: VA Information Security Program*.

2. This Handbook includes VA's privacy controls, which are based on the privacy controls outlined in NIST SP 800-53. These are intended to address the privacy needs across all of VA.

3. This Handbook also provides the criteria to assist management in making governance and integration decisions for VA's security programs.

4. This Handbook represents VA's information technology (IT) overarching security policy that is consistent and in alignment with NIST standards and guidelines and other related requirements set forth in Office of Management and Budget (OMB) memorandums and circulars identified in Appendix C.

6500.2 MANAGEMENT OF BREACHES INVOLING SENSITIVE PERSONAL INFORMATION

VA Publications

Purpose. This Handbook provides oversight, management, and reporting procedures to ensure appropriate and expeditious managing of Privacy breaches involving Sensitive Personal Information (SPI) under the ownership of the Department of Veterans Affairs (VA). This Handbook also contains the criteria that should be used to determine whether a reported incident is a breach involving SPI, and whether VA should notify or offer credit protection services to the record subjects.

6500.5 INCORPORATING SECURITY AND PRIVACY INTO THE SYSTEM DEVELOPMENT LIFE CYCLE

VA Publications

PURPOSE. This Handbook establishes the security and privacy procedures, responsibilities, and departmental framework for incorporating security and privacy in the system development life cycle (SDLC) of information technology (IT) assets that store, process, or transmit Department of Veterans Affairs (VA) information by, or on behalf of, VA as required by the E-Government Act of 2002, Public Law 107-347; to include Title III, The Federal Information Security Management Act (FISMA), and VA Directive and Handbook 6500, Information Security Program.

This handbook is dependent upon the security requirements established in VA Handbook 6500 and other handbooks in the 6500.x series. (see Reference section for a list)

6502 VA Enterprise Privacy Program

VA Publications

Purpose. To update and reaffirm VA Directive 6502, the Department wide program policy for the protection of privacy of veterans, their dependents and beneficiaries, as well as the privacy of all employees and contractors of the Department of Veterans Affairs (VA), and other individuals for whom personal records are created and maintained in accordance with Federal law. This directive clarifies policies, roles, and responsibilities for the VA Privacy Service, also known as the VA Enterprise Privacy Program, the program that oversees all VA-wide privacy programs.

6500.6 Contract Security

VA Publications

GENERAL: Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

6502.3 WEBPAGE PRIVACY POLICY

VA Publications

Purpose. This document outlines general guidelines with regard to creating, posting, and maintaining all Department of Veterans Affairs (VA) Web page privacy policies on the Internet.

The requirements in this document do not extend to non-public VA intranet pages.

While the term “privacy statement” is frequently used, current Office of Management and Budget (OMB) Guidance requires that to promote clarity for the public, all Federal agencies must use the term “privacy policy” when referring to their posted policy statements relating to Web page privacy.

This handbook provides guidance and describes requirements regarding both the

6502.4 PROCEDURES FOR MATCHING PROGRAMS

VA Publications

Purpose. This handbook revises Department-wide procedures for matching programs and describes the process for publishing the notices in the Federal Register.

policy applicable to all VA Web pages (the VA General Web Privacy Policy, or "the general policy"), and policies limited in scope to a particular Web page or set of Web pages. (Limited Web Privacy Policies, or "limited policies").

6508.1 PROCEDURES FOR PRIVACY THRESHOLD ANALYSIS AND PRIVACY IMPACT ASSESSMENT

VA Publications

Purpose. This handbook establishes a detailed methodology for the inclusion of the PTA into the VA enterprise-wide privacy compliance process. In addition, this policy discusses the processes and procedures for the PIA. The PTA is a privacy compliance and risk management tool instrumental in determining whether Personally Identifiable Information (PII) and/or Personal Health Information (PHI) is being collected and maintained by an Information Technology (IT) System, rulemaking, program, and/or project. The PTA facilitates the creation of a privacy risk assessment portfolio maintained by the VA Privacy Service. The PTA and PIA embody the required collaboration of officials in VA programmatic offices, identified in the policy; ISOs, PRIVACY OFFICERs; System Managers/System Owners and the VA Privacy Service.

PII and PHI are subsets of SPI. The term SPI will be used to describe both throughout the policy.

6509 DUTIES OF PRIVACY OFFICER

VA Publications

Purpose. The purpose of this directive is to define the roles of VA Privacy Officers through a hierarchical approach and to connect those roles with the objective of protecting VA's SPI. This methodology will enable Privacy Officers at all levels to accomplish their responsibilities in an efficient and effective manner. When executed, this policy will assist in fulfilling VA's promise to Veterans as well as their dependents and beneficiaries, to protect and properly safeguard their SPI.

6510 VA IDENTITY AND ACCESS MANAGEMENT

VA Publications

Purpose. The Department of Veterans Affairs (VA) has implemented an Identity and Access Management (IAM) Program that provides access to VA information, resources, and services to improve timeliness and promote ease of access for all VA users. VA has established the IAM Business Program Management Office to manage the business of aligning IAM Services to federal mandates and guidance. VA accepts and institutes the policies and guidelines in accordance with the following documents

6511 PRESENTATIONS DISPLAYING PERSONALLY IDENTIFIABLE INFORMATION

VA Publications

Purpose. Many Department of Veterans Affairs (VA) and Veteran Benefit Administration (VBA) presentations and associated materials are shown to non-VA parties and/or are made available for review via the internet or any other public medium. Because these presentations and associated materials may be seen by individuals without a need or authorization to view them, it is imperative that none contain personally identifiable information (PII) or information exempt from release under the Freedom of Information Act of 1966, as amended (FOIA). This Directive outlines requirements to ensure that those VA presentations that are made publicly available do not contain PII or information exempt from release under the FOIA.

This policy only applies to presentations that contain data derived from VA systems that hold or process PII or information exempt from release under FOIA. This policy does not apply to presentations and associated materials that are purely technical in nature or descriptive of a process or program and do not deal with data derived from a VA system that holds or processes PII or information exempt from release under the FOIA. It does not apply to materials used in internal VA meetings where only VA personnel or contractors who are considered a part of the VA workforce are attendance and have a need to know the information for the performance of their official duties. NOTE: Contractors attending VBA meetings where PII or information exempt from release under FOIA is presented must be business associates as defined by the Health Insurance Portability and Accountability Act (HIPAA).

6600 RESPONSIBILITIES OF EMPLOYEES AND OTHERS SUPPORTING VA IN PROTECTING PERSONALLY IDENTIFIABLE INFORMATION (PII)

VA Publications

6609 MAILING OF SENSITIVE PERSONAL INFORMATION

VA Publications

Purpose. This directive supplements existing Department of Veterans Affairs (VA) Directive 6340, Mail Management, by ensuring the protection of the sensitive personal information (SPI) of individuals, including Veterans, dependents, and VA employees. This policy is effective immediately, and is applicable Department-wide to all employees, trainees, contractors, appointees, and volunteers (VA personnel).

The awareness of VA personnel of their individual responsibilities and roles for the protection of SPI is the most essential element of protecting this information, which is vital to the fulfillment of VA's mission. Therefore, it is essential that rules be established for the mailing of SPI, and that these rules be communicated to all VA personnel.

800-53 PRIVACY CONTROL CATALOG APPENDIX J

VA Publications

Purpose. Provides a structured set of privacy controls, based on best practices, that helps organizations comply with applicable federal laws, Executive Orders, directives, instructions, regulations, policies, standards, guidance, and organization-specific issuances: Establishes a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements that may overlap in concept and in implementation within federal information systems, programs, and organizations.

Demonstrates the applicability of the NIST Risk Management Framework in the selection, implementation, assessment, and ongoing monitoring of privacy controls deployed in federal information systems, programs, and organizations; and Promotes closer cooperation between privacy and security officials within the federal government to help achieve the objectives of senior leaders/executives in enforcing the requirements in federal privacy legislation, policies, regulations, directives, standards, and guidance.

38 USC 7332

Title 38 - Pensions, Bonuses, and Veterans' Relief - Code of Federal Regulations (ecfr.io)

Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, Human Immunodeficiency Virus (HIV) Infection, and Sickle Cell Anemia Medical Records, 38 U.S.C. 7332, implemented by 38 CFR Section 1.460-1.496. This statute provides for the confidentiality of certain patient medical record information related to drug and alcohol abuse, HIV infection, and sickle cell anemia and permits disclosure of the protected information only when specifically authorized by the statute.
See definitions document for further explanation of disclosures for drug and alcohol abuse

38 USC 5701

U.S.C. Title 38 - VETERANS' BENEFITS (govinfo.gov)

The VA Claims Confidentiality Statute, 38 U.S.C. 5701, implemented by 38 CFR Section 1.500-1.527. This statute provides for the confidentiality of all VA patient and claimant names and home addresses (and the names and home addresses of their dependents) and permits disclosure of the information only when specifically authorized

by the statute. Title 38 CFR Sections 1.500-1.527 are not to be used in releasing information from patient medical records when in conflict with 38 CFR 1.575-1.584 (Privacy Act), 38 CFR 1.460-1.496 (38 USC 7332), or 45 CFR Parts 160 and 164 (HIPAA).

38 USC 5705

U.S.C. Title 38 - VETERANS' BENEFITS (govinfo.gov)

Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. 5705, implemented by 38 CFR Section 17.500-17.511. This statute provides that records and documents created by VHA as part of a designated medical quality-assurance program are confidential and privileged and may not be disclosed to any person or entity except when specifically authorized by statute.

HIPAA

http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

HIPAA (Public Law (Pub. L.) 104-191) implemented by 45 CFR Parts 160 and 164. This statute provides for the improvement of the efficiency and effectiveness of health care systems by encouraging the development of health information systems through the establishment of standards and requirements for the electronic transmission, privacy, and security of certain health information. VHA must comply with the Privacy rules when creating, maintaining, using, and disclosing Privacy - Home (sharepoint.com)individually identifiable health information.

38 CFR

1.475 Form of written consent.
1.476 Prohibition on redisclosure.
1.477 Disclosures permitted with written consent.
1.478 Disclosures to prevent multiple enrollments in detoxification and maintenance treatment programs; not applicable to records relating to sickle cell anemia or infection with the HIV.
1.479 Disclosures to elements of the criminal justice system which have referred patients.
1.483 Disclosure of information to participate in state prescription drug monitoring programs.
1.485 Medical emergencies.
1.485a Eye, organ and tissue donation.
1.486 Disclosure of information related to infection with the human immunodeficiency virus to public health authorities.
1.487 Disclosure of information related to infection with the human immunodeficiency virus to the spouse or sexual partner of the patient.
1.500-1 Release of Information from Department of Veterans Affairs Claimant Records
1.503 Disclosure of information to a veteran or his or her duly authorized representative as to matters concerning the veteran alone.

1.504 Disclosure of information to a widow, child, or other claimant.
1.507 Disclosures to members of Congress.
1.508 Disclosure in cases where claimants are charged with or convicted of criminal offenses
1.509 Disclosure to courts in proceedings in the nature of an inquest.
1.511 Disclosure of claimant records in connection with judicial proceedings generally.
1.512 Disclosure of loan guaranty information.
1.513 Disclosure of information contained in Armed Forces service and related medical records in Department of Veterans Affairs custody.
1.516 Disclosure of information to undertaker concerning burial of a deceased veteran.
1.517 Disclosure of vocational rehabilitation and education information to educational institutions cooperating with the Department of Veterans Affairs.
1.518 Addresses of claimants
1.519 Lists of names and addresses.
1.521 Special restrictions concerning social security records
1.524 Persons authorized to represent claimants
1.525 Inspection of records by or disclosure of information to recognized representatives of organizations and recognized attorneys.
1.526 Copies of records and papers
1.527 Administrative review.

eCFR :: Title 38 of the CFR -- Pensions, Bonuses, and Veterans' Relief

DEFINITIONS

Agency - Any executive department, military department, government corporation, government-controlled corporation, or other establishment in the executive branch of the Federal government, or independent regulatory entity.

Appeal - A requester's written disagreement with an adverse determination under the FOIA.

Authorized user - Refers to an individual authorized in writing by a competent beneficiary or legally appointed guardian to act for the beneficiary.

Beneficiary - A Veteran or other individual who has received benefits (including medical benefits) or has applied for benefits pursuant to title 38, United States Code.

Benefits records - An individual's records, which pertain to programs under any of the benefits laws administered by the Secretary of Veterans Affairs.

Business day - The time during which typical Federal government offices are open for normal business. It does not include Saturdays, Sundays, or Federal legal public holidays. The term “day” means business day unless otherwise specified.

Business information - Confidential or privileged commercial or financial information obtained by VA from a submitter that may be protected from disclosure under Exemption

Back to top

4 of the FOIA, 5 U.S.C. 552(b)(4).

Complaint - When a Privacy Officer receives information from an individual regarding an alleged violation of the individual's privacy. It may include issues related to impermissible access or disclosure of information covered under any of the privacy and confidentiality laws and regulations pertaining to VA. Access and amendment complaints, which pertain to denial of access and amendment rights, are considered complaints. Complaints are required to be entered into PSETS.

Component - Each distinct VA entity, including Administrations, Program Offices, services, or facilities.

Consent - Permission for something to happen or agreement to do something.

Contractor - Any person contracted to perform services in direct support of VA activities

Expedited processing - Giving a FOIA request priority for processing ahead of other pending requests because VA has determined that the requester has shown an exceptional need or urgency for the records as provided in these regulations.

Fees - For fees and fee-related definitions, see §1.561.

FOIA Office - The individual within a VA component whose responsibilities include addressing and granting or denying requests for records under the FOIA.

Next of Kin - A person's closest living relative or relatives.

Non-Contractor - A regular VA employee.

Non-VA Employee - Select if the person who was responsible for putting information at risk was not a VA employee.

Perfected request - Is when a written FOIA request that meets the requirements set forth in §1.554 of this part and for which there are no remaining issues about the payment of applicable fees or any other matter that requires resolution prior to processing.

Personally Identifiable Information (PII) - Refers to information which can be used to distinguish or trace an individual's identity, such as his/her 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**.**

Privacy Incident - A privacy incident is a privacy or security-related event in which PII may have been exposed through either unauthorized access or disclosure; it includes the loss, theft, or inadvertent misdirection of PII and any other unauthorized access, or any other access other than that which is incidental to the scope of employment, to data containing PII in electronic, printed, or any other format, and results in the potential compromise of the confidentially or integrity of the data regardless of the manner in which the breach might have occurred.

Program Office - Refers to VBA Central Office Lines of Business and Staff Offices. Some Lines of Business exist within VBA Regional Offices that are under the jurisdiction of the Executive Director.

Reading room - A space made available, as needed, in VA components where records are available for review pursuant to 5 U.S.C. 552(a)(2). Ordinarily, the VA component providing a public reading room space will be the component that maintains the record.

Record - A document, a portion of a document, and information contained within a document, and can include information derived from a document or a database. Such documents may be maintained in paper, electronic, and other forms, but do not include objects, such as tissue slides, blood samples, or computer hardware.

Request - A written demand for records under the FOIA as described below. The term request includes any action emanating from the initial demand for records, including an appeal related to the initial demand.

Requester - Generally, any individual, partnership, corporation, association, or foreign or state or local government, which has made a demand to access an agency record.

Sensitive personal information - Refers to claim information that, with a reasonable degree of medical certainty, is likely to have a serious adverse effect on an individual's mental or physical health if revealed to the individual.

Staff Office - Provide direct support to VBA Business lines.

Submitter - Any person or entity (including corporations, state, local and tribal governments, and foreign governments) from whom VA obtains trade secrets or confidential commercial or financial information either directly or indirectly.

Unauthorized access - A person who gains entry to a computer network, system, application software, data, or other resources without permission.

Unauthorized disclosure - Is the communication or physical transfer of classified information or controlled unclassified information (CUI) to an unauthorized recipient.

Unique Identifier – is a value that distinguishes an entity from all others within a given context or system. It is used to ensure each entity can be uniquely identified and distinguished from others.

VA - The Department of Veterans Affairs.**VA Central Office (VACO)** - The headquarters of the Department of Veterans Affairs. The mailing address is 810 Vermont Avenue, NW., Washington, DC 20420.

Written or in writing - Is a communication such as letters, photocopies of letters, electronic mail, and facsimiles (faxes), and does not include any form of oral communication.

ACRONYMS

Everyone in VA uses acronyms. Below are helpful links for the most common acronyms used.

Search for Acronym: VA Acronym Lookup

ADDITIONAL PRIVACY REFERENCES/RESOURCES

Department of Justice http://www.justice.gov/

Health and Human Services Office of Civil Rights HIPAA Home | HHS.gov

VA Privacy Service VA Privacy Service Privacy Hub - Home (sharepoint.com)

VA Office of Information Security Office of Information Security - Careers in IT (va.gov)

VBA Privacy Services Home - Privacy

VBA Incident Resolution: DBRS SharePoint site

VA Freedom of Information Act: Freedom of Information Act (va.gov)

VA DIRECTIVES and HANDBOOKS

VA Specific Privacy Policies

- VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act
- VA Handbook 6300.5, Procedures for Establishing and Managing Privacy Act System of Records
- VA Directive 6500.2, Management of Security and Privacy Incidents
- VA Directive 6502, Privacy Program
- VA Handbook 6500, Information Security Program
- VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment
- VA Handbook 6508.1, Privacy Impact Assessment (PIA)
- VA Directive 6509, Duties of Privacy Officers
- VA Directive 6511, Presentations Displaying Personally Identifiable Information
- VA Directive 6609, Mailing of Sensitive Personal Information

VA Publications VA Publications
VA Forms VA Forms

Back to top

There are eight privacy control families, each aligning with one of the FIPPs. The privacy families can be implemented at the organization, department, agency, component, office, program, or information system level, under the leadership and oversight of the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)122 and in coordination with the Chief Information Security Officer, Chief Information Officer, program officials, legal counsel, and others as appropriate.

Table J- 1 provides a summary of the privacy controls by family in the privacy control catalog.

TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY

ID	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice

Back to top

TR-1	System of Records Notices and Privacy Act Statements
TR-1	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Back to top

Appendix 1
Alphabetized Content List

Back to top

Back to top

Back to top

Appendix 2

DEPARTMENT OF VETERANS AFFAIRS
Veterans Benefits Administration
Washington, D.C. 20420

February 24, 2023

VBA Letter 20-23-02

Director (00)

All VBA Services, District Offices, Regional Offices, Program Offices, and Centers SUBJ:

VBA Privacy Program Implementation

PURPOSE

This letter rescinds VBA Letter 20-19-09, Release of information from a Privacy Act (5 U.S.C. § 552a) System of Records, dated September 27, 2019. It provides updated guidance for all Veterans Benefits Administration (VBA) District Offices, Regional Offices, Service Offices, Program Offices, and Centers on the release of information from Privacy Act Systems of Records (SORs). This guidance change is effective upon issuance of this letter.

SUMMARY OF CONTENT

This letter provides guidance on the disclosure of records subject to the Privacy Act of 1974. The Privacy Act prohibits the disclosure of information contained in a SOR absent a written request by or with the prior written consent of the subject individual to whom the record pertains unless the disclosure is pursuant to one (1) of the twelve (12) statutory exceptions stated in the statute as described below. VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, implements the statutory language.

AUTHORITY

5 U.S.C. § 552a, Privacy Act of 1974, implemented by 38 C.F.R. §§ 1.575-1.582 5 U.S.C. § 552, Freedom of Information Act (FOIA), implemented by 38 C.F.R. §§ 1.550-562
38 U.S.C. § 5701, Confidential nature of claims, implemented by 38 C.F.R. §§ 1.500-1.527
38 U.S.C. § 7332, Confidentiality of certain medical records, implemented by 38 C.F.R. § 1.460-1.496

Back to top

BACKGROUND

The Privacy Act establishes a code of fair information practices that govern the collection, maintenance, use, and dissemination of Personally Identifiable Information (PII) about United States citizens or lawfully admitted permanent resident aliens (hereinafter referred to as “individual”) in SORs generally maintained by an agency in the executive branch. The Privacy Act also allows individuals a right to access records about themselves contained in SORs, requiring agencies to provide an individual, upon request, an opportunity to review their Privacy Act records and have a copy made of all or any portion of the records. In addition, the Privacy Act provides the right to individuals to request an amendment of their Privacy Act records which they believe are inaccurate, irrelevant, untimely, or incomplete, and an accounting of disclosures made to any person or entity outside the agency during the previous five years.

In addition to the Privacy Act, two statutes also protect the confidentiality of VA claimants’ records. The provisions of 38 U.S.C. § 5701, Confidential nature of claims, provide for additional confidentiality and must be met prior to releasing any VA claimant’s records. The provisions of 38 U.S.C. § 7332, Confidentiality of certain medical records, protect information related to VA’s treatment of individuals for drug abuse, alcoholism or alcohol abuse, HIV/AIDS, and sickle-cell anemia.

Exceptions to Prohibition Against Disclosure Without Consent

The Privacy Act prohibits the disclosure of information from a SOR absent the subject individual’s written consent unless the disclosure is pursuant to any of the twelve (12) statutory exceptions to the general prohibition against release. The exceptions to the written consent rule, which permit an agency to release an individual's Privacy Act records without their consent, include disclosure:

1. To those officers and employees of the agency who have a need for the record in the performance of their duties under Exception (b)(1).
2. As required by the Freedom of Information Act (FOIA), under Exception (b)(2).
3. Under a routine use as outlined in the System of Records Notice (SORN), under Exception (b)(3).
4. To the Bureau of the Census for purposes of planning or carrying out a census, survey, or related activity, under Exception (b)(4).
5. To a recipient who has provided advance written assurance that the record will be used solely as statistical research or reporting record and transferred in a form that is not individually identifiable, under Exception (b)(5).
6. To the National Archives and Records Administration as a record that has sufficient historical or other value to warrant its continued preservation or evaluation, under Exception (b)(6).
7. To another agency or to an instrumentality of any governmental jurisdiction under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality

Back to top

has made a written request to the agency which maintains the record specifying the particular portion desired, and the law enforcement activity for which the record is sought, under Exception (b)(7).
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 such individual, under Exception (b)(8).
9. To either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress, or subcommittee of any such joint committee, under Exception (b)(9).
10. To the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the Government Accountability Office, under Exception (b)(10).
11. Pursuant to the order of a court of competent jurisdiction, under Exception (b)(11).
12. To a consumer reporting agency in accordance with § 3711(e) of Title 31, under Exception (b)(12).

First-Party Access to One's Own Records

A first-party request is a request in which an individual seeks access to records about themselves. The Privacy Act requires an agency to provide the subject individual of a record with access to or a copy of their own record upon request. The request must:

1. Be in writing, signed, and dated
2. Reasonably describes the record(s) being requested and the name of the VBA SOR where the records are stored, if known.

While not required, VBA encourages using approved authorization forms to request access to records. A list of approved authorization forms is included in this letter. If a requester chooses not to use an authorization form, the above-outlined requirements must be met.

VA must provide the first-party requester with:

- A copy of all files or a particular record about the subject individual and maintained in a SOR, such as a copy of their entire or partial VA claims folder, Electronic Folder (eFolder), Vocational Rehabilitation plan, or correspondence sent to the individual's member of Congress; or
- An opportunity for the individual to visit the regional office to review their own record(s).[1]

If third-party information is identified within the record, further analysis is required (see the section on Access to Third-Party Information Within Privacy Act Records).

[1] C.F.R. §1.500(a) allow personal contact at a facility during normal duty hours to access or obtain records from a SOR.

Back to top

If any one of the ten Privacy Act exemptions to the right of access apply to the records, then the records should not be released.[2] The following two VBA SORs contain specific exemptions from the Privacy Act provisions on access, amendment, and other requirements:

- Loan Guaranty Fee Personnel and Program Participant Records (SORN 17VA26); and
- Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records, Specially Adapted Housing Applicant Records, and Vendee Loan Applicant Records (SORN 55VA26).

Please consult your Privacy Officer to obtain further guidance on responding to requests for copies of records contained in these systems.

If the records are not released because a Privacy Act exemption applies to the request, the request must be processed under the FOIA before a final release determination is made.

Identification of Requester

Identification of the individual requesting the information is required and will consist of the requester's name, signature, address, and claim, insurance, or other identifying file number, if any, as a minimum.

NOTE: The Privacy Act right of access may be exercised on behalf of the subject individual by a duly authorized representative, such as an accredited attorney, agent, or representative of a Veteran Service Organization (VSO). Such requests should be treated as a first-party request. A requester may use approved VA authorization forms to designate such persons (e.g., VA Form 21-0845). However, an approved VA form is not required, so long as the letter of designation is signed by the subject individual and sufficiently describes the authority being provided to the representative.

Access to Third-Party Information Within Privacy Act Records

Although first-party requesters are entitled to their own non-exempt Privacy Act records, they are not necessarily entitled to information about a third-party that does not pertain to them.

An individual's Privacy Act records may contain information pertaining to other persons, such as PII of dependents, other Veterans, or healthcare providers. Some of these records originated from the Department of Defense (DoD), where service member lists with PII of multiple service members were filed within individual service members'

[2] The Privacy Act contains exemptions which exclude a SOR from one or more of the provisions, such as an individual's right of access or amendment. The list of exemptions can be found at https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/exemptions.

Back to top

records, and healthcare providers' SSNs were used as identifiers. Such records may also include constructive claims folders of spouses and children; promotion rosters; military records; and medical records containing SSNs, names, and other PII of a person who is not the subject of the request.

If third-party information within a responsive document is considered not to be part of the requester's Privacy Act record, i.e., it is not about the requester, that information should be processed under the FOIA. In this case, the response letter should explain to the requester that certain information responsive to their request consists of third-party information that does not pertain to them and to which they do not have access under the Privacy Act.

NOTE: Records released pursuant to a first-party request for an individual's own records from a non-exempt SOR must not contain any combination of PII of other individuals which may lead to the identification of a specific individual. Therefore, such records must be reviewed by a designated government employee prior to release to ensure appropriate redaction and removal of third-party information.

NOTE: An accurate record must be kept of information withheld as Third-Party Information to enable review of administrative appeals by the Office of General Counsel. This should consist of a copy of the records as released or a detailed index of information withheld.

38 U.S.C. §7332 Protected Information

VBA must have the legal authority to disclose 38 U.S.C. § 7332-protected information which includes:

1. Treatment for drug abuse
2. Alcoholism or alcohol abuse
3. HIV status
4. Sickle cell anemia

Authority to disclose 38 U.S.C. § 7332-protected information may be provided on an approved VA authorization form signed by the subject individual or through signed written consent via letter, affidavit, etc. If there is no legal authority to disclose it, this information must be withheld via redaction.

NOTE: As noted above, records protected under 38 U.S.C. § 7332 require a special authorization consistent with 38 C.F.R. § 1.475. While VA Form 3288, Request for and Consent to Release of Information from Individual's Records, permits VA to release an individual's Privacy Act records, it does not allow the blanket release of § 7332- protected records under VA regulations. Form 3288 must explicitly include language authorizing the release of this information. If authorization is deficient for such disclosure, VA may ask the individual, but not the requester, to provide a § 7332-

Back to top

compliant consent.

Third-Party Requests for Privacy Act Records

Third-party requests for Privacy Act records should be processed only under the FOIA. Third parties do not have right of access to records under the Privacy Act, so their only potential right of access comes from the FOIA.

Requests for Deceased Veterans' Records

Records of deceased individuals are not protected by the Privacy Act and do not require a Privacy Act exception for release to next of kin with the request. Requests for deceased Veterans' records are FOIA requests. Because deceased individuals have no recognizable privacy interest, records are only subject to withholding under FOIA Exemption (b)(6) where information may impact surviving relatives or family members. Information about living persons maintained in a deceased Veteran's file may require redaction under Exemption (b)(6) when processed under FOIA. The names and addresses of deceased Veterans may be redacted under Exemption (b)(3) as confidential under the provisions of 38 U.S.C. § 5701, Confidential Nature of Claims.

NOTE: Records that contain § 7332 information may be released to the next-of-kin of a deceased Veteran only for the purpose of obtaining survivorship benefits or with the authorization of the administrator, executor, or other court-appointed representatives of the deceased Veteran's estate.

Amendment of Records

Under the Privacy Act, an individual has the right to request an amendment of their own records retrieved by their name, claim number, or other identifiers. An amendment request must:

- be in writing,
- be signed,
- adequately describe the specific information the individual believes to be:
    - Inaccurate (i.e., faulty, or not conforming exactly to truth).
    - Incomplete (i.e., unfinished, or lacking information needed).
    - Irrelevant (i.e., inappropriate, or not pertaining to the purpose for which records were collected).
    - Untimely (i.e., before the proper time or prematurely),
    - and include the reason for this belief.

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

Back to top

The process for amendment of records must be documented in a system's published SORN.

Accounting of Disclosures

The Privacy Act requires an agency to maintain a list of all disclosures made from a subject individual's record to persons or entities outside of VA. The publishing of a system SORN in the federal register and the 12 Exceptions to the prohibitions against disclosure outlined above represent notification to subject individual regarding how and to whom VA may share their information. However, VA must provide the individual, upon request, an accounting of all such disclosures which include:

- The date, nature, and purpose of the disclosure; and
- The name and address of the person or entity to whom the disclosure was made.

VA is required to provide an accounting of disclosure for any period requested within the previous five years.

An accounting is not required for releases:

- To the subject individual in response to a first-party access request to their own records.
- To those officers and employees of the agency who have a need for the record in the performance of their official duties, under the need-to-know exception of Exception (b)(1); or
- A FOIA request, under Exception (b)(2).

FOIA/Privacy Act (FP) Request Tracking

In order to maintain transparency and openness, VBA utilizes FOIAXpress (FX) as its official tracking system for FOIA/Privacy Act (FP) requests. All requests that meet requirements for withholding third-party information under the FOIA must be tracked in FX. The following documents are to be uploaded into FX:

- Initial request
- Acknowledgement letter
- Correspondence (i.e., emails and attachments)
- Final response letters (initial agency decision)

Responsive records (e.g., claims files) are not to be uploaded into FOIAXpress. However, as noted above a complete administrative record must be kept of any information that is withheld as third-party information to enable administrative review.

Back to top

NOTE: Privacy Act requests that do not require redactions of third-party information under the FOIA are not to be tracked in FOIAXpress.

VBA Privacy Program Guidance

As outlined within VA Directive 6509, Duties of Privacy Officers, (2)(a) Policy-VBA Administration, staff, and regional (VBA) offices must each designate a Privacy Officer and an Alternate Privacy Officer to ensure compliance with privacy laws, guidance from the Office of Management and Budget, the National Institute of Standards and Technology Security and Privacy Controls, VA, and VBA guidance. Any updates to the designation should be reported via email to the VBA Privacy Office at privacy.vbavaco@va.gov as soon as the information becomes available.

In cases where records requests are fulfilled via postal mail, they must be sent in accordance with VA Directive 6609, Mailing of Sensitive Personal Information.

DEFINITIONS

Individual – a citizen of the United States or an alien lawfully admitted for permanent residence.

Next-of-Kin – defined as any of the following: the un-remarried widow or widower, son, daughter, father, mother, brother, or sister of the deceased veteran. Next-of-kin must also provide proof of death of the veteran, such as a copy of the death certificate, a letter from the funeral home or a published obituary.

Record – any item, collection, or grouping of information about an individual which is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that contains their name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph within a SOR.

Routine Use – with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

System of Records (SOR) – a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying information assigned to the individual.

System of Records Notice (SORN) – A SORN is a formal notice to the public, published in the Federal Register, that an agency is maintaining information about individuals and identifies the purpose for which such information is collected, from whom and what type of PII is collected, how the PII is shared externally through routine

Back to top

uses, and how to access and correct any such information maintained by the Department.

Personally Identifiable Information (PII) – 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 (e.g., covered by the Privacy Act) to be PII. Please see VA Handbook 6500 for additional information.

APPROVED AUTHORIZATION FORMS

Approved authorization forms may be used to make Privacy Act requests. However, an approved authorization form is not required. A Privacy Act request may be submitted in any format but must be signed by the requester, or, in the case of a request on behalf of a Veteran, a signed authorization from the Veteran.

1. **VA Form 3288**, *Request for and Consent to Release Information from Claimant's Records*
2. **VA Form 21-4138**, *Statement in Support of Claim*
3. **VA Form 20-10206**, *Freedom of Information Act (FOIA) or Privacy Act (PA) Request*
4. ***VA Form 21-0845***, *Authorization to Disclose Personal Information to a Third Party*
5. **SF-180**, *Request Pertaining to Military Records*

REFERENCES

Privacy Act 1974 (5 U.S.C. § 552a)
38 USC § 5701, *Confidential Nature of Claims*
38 USC § 7332, *Confidentiality of Certain Medical Records* **VA Directive 6609**, *Mailing of Sensitive Personal Information* **VA Directive 6509**, *Duties of Privacy Officers*
VA Handbook 6300.4, *Procedures for Processing Requests Subject to the Privacy Act*
VA SORN Database

Back to top

RESPONSIBLE OFFICE

If you have questions regarding this guidance, contact the VBA Privacy Office, Office of Mission Support (20M33) at privacy.vbavaco@va.gov.

/s/

Joshua Jacobs
Senior Advisor for Policy,
Performing the Delegable Duties of the Under Secretary for Benefits

Back to top