Privacy Impact Assessment for the VA IT System called:

Printing of Unidentified Records (PUR)

Veterans Benefits Administration (VBA)

Office of Information Technology

eMASS ID # 2328

Date PIA submitted for review:

10/15/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.Harvey@va.gov	202-461-8401
Information System Security Officer	Joseph Facciolli	Joseph.Facciolli@va.gov	215-842-2000 x2012
Information System Owner	Christina Lawyer	Christina.Lawyer@va.gov	518-210-0581

Abstract

The abstract provides the simplest explanation for "what does the system do?".

The Printing of Unidentified Records (PUR) application exists to help reconcile physical Veteran mail that is unable to be associated with a specific Veteran for various reasons. That could include situations such as mail that is received by the VA by a veteran with incomplete identifying information or by a member of the public that has received mail unintentionally and sent to the VA via "return to sender". The system will ingest this mail, send out new mail packets with instructions on rectifying the situation and/or attempting to collect the information in question, and when there is enough information for the mail items in question to be tied to a specific veteran, be linked to that veteran's eFolder.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?
Printing of Unidentified Records – Office of Information Technology

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
PUR is an automated component of the Veterans Benefits Management System (VBMS) designed to accept unidentified mail that is received by the VA and has a valid return address. When PUR receives unidentified mail, the process creates an Instruction Letter that is returned along with a scanned copy of the original mail back to the sender. The intention is that the sender completes the Instruction Letter and mails it back to the VA; the additional information collected on the Instruction Letter will aid the VA in identifying the Veteran to the mail. Once the mail is associated to a Veteran, the mail can be moved to the Veteran's eFolder. There are 2 primary processes associated with the automated portion of the PUR system: Unidentified Mail process, and the Identified Mail process.

The Unidentified Mail process occurs once unidentified mail is scanned and received by the PUR application. Unidentified mail that is received and has a valid return address is marked with a QR code containing a Unique Identifier (PUR Unique ID) and redistributed back to the sender with an Instruction Letter that requests additional information to identify the Veteran.

The Identified Mail process occurs when mail received by the VA (that was previously unidentified) is received again and identified through PUR processing and resubmission

with an identifying PUR Unique ID. Once the PUR Unique ID is matched to all previously received mail, then all received documents are moved to the Veteran's eFolder.

C. Who is the owner or control of the IT system or project?
PUR is VA owned and VA operated.

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?
Typical individuals with information in this system are Veterans or individuals who have submitted pieces of mail pertaining to a veteran to the VA. The projected number of individuals whose information is stored within this system is an average of 54000 over the course of 3 years.

E. What is a general description of the information in the IT system and the purpose for collecting this information?
Information in this system includes the following elements of metadata associated to pieces of unidentified mail awaiting reconciliation to a veteran's eFolder:

- PUR Unique ID
- Centralized Mail Packet ID
- Name
- Personal Mailing Address
- File ID
- Integrated Control Number (ICN)
- Electronic Data Interchange
- Personal Identifier (EDIPI)
- Social Security Number
- Participant ID
- File Name

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.
Document Generator (DocGen): Used to generate an instruction letter that will be sent to the original sender.

Veteran Enterprise File Storage (VEFS) Claim Evidence: Provides upload and download functionality for the unidentified-mail bin.

Centralized Mail Portal (CMP): The Centralized Mail Portal (CMP) receives unidentified mail and submits unidentified mail to Claim Evidence. CMP also submits mail that has a PUR Unique ID that is still unidentifiable to Claim Evidence.

Centralized Benefits Communication Management (CBCM): Provides a service to distribute outgoing mail to the sender of the unidentified mail.

Mail Automation Services (MAS): This organization consumes the PUR Identified mail endpoint to submit correspondence received from a sender, whose mail is identifiable

with a PUR Unique ID. When mail is received that has been marked with a QR encoded PUR Unique ID and is identifiable they consume the PUR Identified Mail endpoint.

G. *Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?*
Printing of Unidentified Records resides within the Veterans Administration Enterprise Cloud (VAEC) which is hosted within Amazon Web Services (AWS). This environment and access control ensures accessibility and provides data integrity and consistency across all sites used to access the application through the VA network.

3. Legal Authority and SORN

H. *What is the citation of the legal authority to operate the IT system?*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021)
VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*
The SORN will not require amendment or revision. The current SORN covers cloud usage and storage.

4. System Changes

J. *Will the completion of this PIA will result in circumstances that require changes to business processes?*
Completion of this PIA is not expected to result in a change to business processes.

K. *Will the completion of this PIA potentially result in technology changes?*
Completion of this PIA is not expected to result in technology changes.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account Numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☒ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements: PUR Unique ID, Centralized Mail Packet ID, Uploading User Name, File ID, Electronic Data Interchange Personal Identifier (EDIPI), Participant ID, File Name

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

PII Mapping of Components (Servers/Database)

Printing of Unidentified Records consists of 4 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Printing of Unidentified Records and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
PUR Database (DB)	No	Yes	• PUR Unique ID • Centralized Mail Packet ID • Name • Upload User Name	Identification and Reconciliation of mail item to Veteran eFolder	Encryption at rest, encryption in transit via Secure Sockets Layer (SSL) mutual TLS
PUR Application Programming Interface (API)	Yes	No	• Name • Personal Mailing Address • File ID • ICN • EDIPI • Social Security Number • Participant ID	PUR API integrates with Claim Evidence to store and retrieve files	Representational State Transfer (REST) web service API Hypertext Transfer Protocol Secure (HTTPS)
PUR DG (docgen plugin)	No	No	• Name • Personal Mailing Address	DocGen services are used to generate the Unidentified Mail Instruction Letter.	REST web services API (HTTPS)

Claim Evidence DB	No	Yes	• Name	File storage for files uploaded via CMP	Encryption at rest, encryption in transit via (SSL) mutual TLS

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

PUR receives data from unidentified mail that originates with either a veteran or an individual sending information regarding a veteran.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Because the mail items in question are unreconciled, there is a potential that someone other than a veteran may be submitting the information. There is also a chance that the individual submitting may not be associated directly with the veteran for whom the mail relates.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

PUR creates a unique ID consisting of a globally unique identifier (GUID) that is then attached to the unidentifiable mail item in question.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Information is collected via mail items received by the VA or VA mail vendor and ingested via the Central Mail Portal.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

Information is not collected on a form.

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Information stored within the Printing of Unidentified Records (PUR) system is not checked against other sources. Mail Automation Services does validate the address before consuming our service. When an unidentified mail packet is submitted to the PUR system from Mail Automation, PUR logs the event and creates an instruction letter that is returned to the sender so that the mail received can be identified to a veteran. PUR does not identify the mail to a veteran.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

PUR does not conduct accuracy checks by accessing a commercial aggregator of information.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021)
VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: Pieces of mail could be associated with a Veteran for which that mail does not match.

Mitigation: Pieces of mail are applied with a unique identifier. Only at a time when sufficient data is received that confirms Veteran Identity will the previously-unidentified mail be associated to the Veteran and moved into that Veteran's Claim Evidence eFolder.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
PUR Unique ID	Tag unidentified mail for tracking and association to Veteran	Tag unidentified mail for tracking and association to Veteran
Centralized Mail Packet ID	Tracking of unidentified mail item	N/A
Name	Used for populating the instruction letter.	Used for populating the instruction letter.
Uploading User Name	Metadata acquired as part of mail intake	N/A
File ID	Tracking of mail item	Tracking of mail item
Integrated Control Number (ICN)	Veteran Identifying Information	N/A
Electronic Data Interchange Personal Identifier (EDIPI)	Veteran Identifying Information	Veteran Identifying Information

Social Security Number	Veteran Identifying Information	Veteran Identifying Information
Participant ID	Veteran identifying Information	N/A
File Name	Tracking of unidentified mail item	N/A
Personal Mailing Address	Populating and mailing instruction letter	Populating and mailing instruction letter

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

PUR does not conduct any type of analysis.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

PUR does not make available new or unutilized information about an individual.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

All sensitive and confidential data is encrypted using Federal Information Processing Standard (FIPS)140-2 compliant AES-256 encryption algorithms in transit and at rest. The information includes objects in VAEC AWS GovCloud s3 buckets, Elastic Block Store (EBS) volumes, and databases. AWS uses EBS encryption (AES-256 algorithms) which uses AWS Key Management Service keys when creating encrypted volumes and snapshots.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

The protections listed above in 2.3a apply here as well.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

Data is stored in a secure enclave within AWS. Access to information is protected by industry standard authentication and authorization protocols. Data is encrypted both in transit and at rest.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Access to PII is determined through the use of RBAC (rules-based access control) through the following:
• Common Security Services (CSS) – UI login of the application
• RedHat Identity Management (IdM) – application container logs
• VA Active Directory – AWS Console Access

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the ROB, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

2.4c Does access require manager approval?

Yes

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes, Automated User account management occurs at multiple levels with respect to BIP (Benefits Integration Platform) that hosts this application due to the layered architecture and

implementation of services upon the platform. BIP currently employs Red Hat IdM (Identity Management) to support the management of information systems accounts.

All access to PII data is being logged to centralizing logging and monitoring via AWS OpenSearch.

2.4e Who is responsible for assuring safeguards for the PII?

As a containerized application hosted on BIP, the BIP Accelerator team controls the security safeguards that are in all applications utilizing BIP's Framework.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

- PUR Unique ID
- Centralized Mail Packet ID
- Name
- Upload User Name

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. **The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.** If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Data is retained indefinitely based on VA guidance as this data could involved the processing of claims for Veterans and their dependents. To ensure these benefits are received, retention of this documentation is critical.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the

proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes

3.3b Please indicate each records retention schedule, series, and disposition authority?

These records are retained and disposed of in accordance with the General Records Schedule 3.2: Information Systems Security Records and 4.2: Information Access and Protection Records, approved by National Archives and Records Administration (NARA). https://www.archives.gov/records-mgmt/grs.html

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

All paper documentation that is not the property of VA (e.g., DoD-owned documentation) is currently stored by VA after scanning, pending a policy determination as to its final disposition. All documentation being held pursuant to active litigation is held in its native format during the pendency of the litigation. All VBMS eFolders are stored on a secure VA server, pending permanent transfer to NARA where they will be maintained as historical records. Once an electronic record has been transferred into NARA custody, the record will be fully purged and deleted from the VA system in accordance with governing records control schedules using commercial off the shelf (COTS) software designed for the purpose. Once purged, the record will be unavailable on the VA system, and will only be accessible through NARA. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

PII is not used for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: Potential risk of data leak may exist with retaining personal data for any amount of time. Mitigation steps below will reduce this kind of attack surface.

Mitigation: Controlled access to the data is maintained with adherence to the principle of minimalization. Only those personnel required by job assignment have access to the data. Each employee with access to the data is required to attend data privacy training.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Document Generator (DocGen)	For creation of the instruction letter to be sent as part of the process to tie unidentified mail to a particular veteran	• Name • Personal Mailing Address	REST web service API (HTTPS)
VEFS Claim Evidence	For management of document transfers into the veterans eFolder	• File Name • File ID	REST web service API (HTTPS)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining SPI is that this data may be disclosed to individuals who do not require access which would increase the risk of the information being misused.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA

Employees and include employee security and privacy training along with required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT	***List the purpose of information being shared / received /***	***List the specific PII/PHI data elements that are processed***	***List the legal authority,***	***List the method of transmission***

System information is shared/received with	***transmitted with the specified program office or IT system***	***(shared/received/transmitted)with the Program or IT system***	***binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***and the measures in place to secure data***
Centralized Mail Portal (CMP)	Centralized Mail Portal (CMP) receives unidentified mail and submits unidentified mail to Claim Evidence. CMP also submits mail that has a PUR Unique ID that is still unidentifiable to Claim Evidence.	• Name • Personal Mailing Address • File ID	MOU/ISA	REST web service API (HTTPS)
Centralized Benefits Communication Management (CBCM)	Provides a service to distribute outgoing mail to the sender of the unidentified-mail.	• Name • Personal Mailing Address • File ID	MOU/ISA	REST web service API (HTTPS)
Mail Automation Services (MAS)	MAS submits correspondence whose mail is identifiable with a PUR Unique ID	• PUR Unique ID • File Number • EDIPI • Social Security Number	MOU/ISA	REST web service API (HTTPS)

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: PII, including personal contact, service, and/or benefits information, could be released to unauthorized individuals. Additionally, misspelling a Veteran's name could result in the wrong data being displayed to the user.

Mitigation: Outside agencies provide their own level of security controls such as access control, authentication, and user logs in order to prevent unauthorized access. The ISA/MOUs between PUR and external agencies establish the security requirements for the VA and the external agency. The security controls identified by NIST SP 800-53 for a moderate system are implemented to protect PUR and external agencies.

All personnel with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior (ROB) annually. PUR users and applications adhere to all information security requirements established by VA OIT, and information is shared in accordance with VA Handbook 6500. All personnel accessing Veteran's information must first have a successfully adjudicated fingerprint check conducted by the Federal Bureau of Investigation (FBI). Individual users are given access to Veterans' data through the issuance of a user ID and password and using a Personal Identity Verification (PIV) card for two-factor authentication.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Notice was provided under…

System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021)
VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
Notice was provided under…
System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021)
VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.
The Department of Veterans Affairs provides public notice that the system exists in two ways:
1. The System of Record Notice listed in the Federal Register:
System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021)
VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

2. This Privacy Impact Assessment (PIA) also serves as notice as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." The PIA can be found at the following PIA Web Site Address: https://department.va.gov/privacy/privacy-impact-assessments/

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.
Responding to information collection is voluntary. However, if information is not provided, then pending or ongoing benefits may be denied or delayed to the veteran for which these mail items contribute to.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent

is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.
Veterans and Service Members may decline or request that their information not be included as part to determine eligibility for benefits. No penalty or denial of service is attached with not providing needed information; however, services may be delayed.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: A risk exists that members of the public are not aware of the PUR system within the Department of Veterans Affairs and that their information is/could be used by the system.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists including the Privacy Impact Assessment and a System of Record Notice.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Procedures are outlined in…
System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021)

VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The system is not exempt from the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

This system is a privacy act system and as such any individual who wishes to determine whether a record is being maintained under his or her name in PUR, or wishes to determine the contents of such records, should submit a written request or apply in person to the VA facility where the records are located. For a directory of VA facilities and phone numbers by region, see https://www.benefits.va.gov/benefits/offices.asp.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Procedures are outlined in…
System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021)
VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Notification is provided in the…
System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021)
VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Procedures for redress and amendment are outlined in…
System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021)
VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that information about an individual within the system is incorrect and the individual does not have the information necessary to go about disputing or addressing the inaccuracies.

Mitigation: This PIA as well as the SORN both document avenues available to gain access to, redress, and make corrections to their information.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

Access to the system is requested utilizing Electronic Permission Access System (ePAS). Users submit access requests based on their individual need to know and job duties. Their Supervisor, ISO (Information System Owner) and OI&T (Office of Information & Technology) approval must be obtained prior to access being granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination (two-factor authentication is enforced). Once inside the system, individuals are authorized to access information on a need-to-know basis.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Users from outside the VA do not have access to the system.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Users must be registered in CSUM (Common Security User Management), a VA internal application. Access to information is based on application user roles for access to the information. The primary users of the PUR application are Central Office Representatives (CO Rep) and the Unidentified Mail Sender. The CO Rep is a VBA user within the role of CO Rep, who therefore holds special associated role credentials. These credentials allow a CO Rep user to see the PUR Unidentified Mail Dashboard within VBMS and resend any "failed" distribution from this dashboard. Each VBA user of the PUR application will be given the assigned credentials of a CO Rep for utilization. The Unidentified Mail Sender is the person submitting mail to the VA Compensation and Pension (C&P) office that is unable to be identified.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

There is a Benefits Integrated Platform (BIP) NDA in place. It covers all personnel working on PUR. The PUR development team is comprised of VA personnel and contractors. Access to PUR is required for system administrators and developers for day-to-day maintenance of

the systems and networks. Review of access to PUR is performed on a quarterly basis by the Information System Owner (ISO) and the security engineer. Clearance is required for each person accessing the system. Contracts are reviewed annually by the Contracting Officer's Representative (COR). VA OIT provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users when required by system changes and annually thereafter.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System 2.0 (TMS). After the user's initial acceptance of the ROB, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 2.0 system.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 10/30/2023
3. *The Authorization Status:* Assess Only - Approved
4. *The Authorization Date:* 05/08/2024
5. *The Authorization Termination Date:* 05/08/2026
6. *The Risk Review Completion Date:* 05/08/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)*

PUR utilizes the (SaaS) Software as a Service model within the VA Enterprise Cloud (VAEC) | AWS WebGov Cloud.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

Section 10. References

Summary of Privacy Controls by Family

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-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
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

MARVIS HARVEY

Digitally signed by MARVIS HARVEY
Date: 2024.11.20 12:12:15 -06'00'

Privacy Officer, Marvis Harvey

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2024.11.07 12:03:29 -05'00'

Information System Security Officer, Joseph Facciolli

CHRISTINA LAWYER

Digitally signed by CHRISTINA LAWYER
Date: 2024.11.07 13:50:58 -05'00'

Information System Owner, Christina Lawyer

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021)
VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices