Privacy Impact Assessment for the VA IT System called:

Automated Benefits Delivery - Virtual Regional Office (ABD-VRO)

Veterans Affairs Central Office (VACO)

Chief Technology Officer (OIT-005E)

eMASS ID # 2143

Date: 6/4/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lakisha Wright	lakisha.wright@va.gov	202-632-7216
Information System Security Officer (ISSO)	Jeffery Gardiner	jeffrey.gardiner@va.gov	919-286-0411
Information System Owner	Emily Theis	emily.theis@va.gov	224-803-0968

Abstract

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

Automated Benefits Delivery - Virtual Regional Office (ABD-VRO) is a custom-developed software platform developed by the VA Office of the CTO (OCTO), that enables development teams to quickly build software to improve the VA's internal claims process. ABD-VRO provides deployment and data services to development teams, with the data services leveraging APIs and data streams from other VA systems. ABD-VRO is hosted on the VA Enterprise Cloud and operates under VA's Lighthouse Delivery Infrastructure LHDI ATO.

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?

The system is called Automated Benefits Delivery - Virtual Regional Office (ABD-VRO), built and maintained by the Office of the Chief Technology Officer (OCTO) in partnership with the Veterans Benefits Administration (VBA) as the key business stakeholder.

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

The purpose of the system is to provide technologies that accelerate the disability benefit adjudication process to reduce the time it takes to provide Veterans with a decision.

C. Who is the owner or control of the IT system or project?

The ABD-VRO system is deployed as a tenant within the Lighthouse Delivery Infrastructure (LHDI) platform owned by the Office of Information Technology (OIT) and falls under LHDI's ATO. It will be maintained under the control of OCTO.

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?

ABD-VRO stores data related to the processing of claims (as described in 2E), and in that respect the information stored on the system will contain reference IDs to individuals; however, these reference IDs are not PII, and the system otherwise does not store information about individuals. ABD-VRO is involved in the processing of

approximately 300 claims per month. The typical client is a Veteran or a representative working on their behalf to file a disability claim.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

The information is related to the processing of claims - for example, information on when a claim is opened, closed, or last updated and the nature of the claim, for example, the disability condition and disability rating. The purpose for collecting this information is so that business logic built in VRO can perform analysis and detect situations where a step of the claim processing workflow can be performed programmatically, in which case VRO coordinates the appropriate API requests.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

Representative modules that share information:

The Max Claim for Increase (CFI) module exposes through an API endpoint the max disability rating for a given disability condition. This data is consumed by a service on VA.gov.

The End Product (EP) Merge module identifies claims that can be merged and automates that function so that a claims processor does not manually need to intervene. VRO uses BIP and BGS APIs to perform the merging and annotation, which might be considered information sharing between BIP and BGS, both VA systems.

The Contention Classifier module has a feature that exposes through an API endpoint a feature to link claims in VA.gov and VBMS to each other, in order to track contention changes downstream. This linking might be considered information sharing within VA systems. The target user for this module is Performance Analysis & Integrity (PA&I).

The VRO system facilitates the sharing of data and falls within the scope of the examples described above.

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?

The system is operated solely within the LHDI platform which itself is operated within the VA Enterprise Cloud (VAEC).

3. Legal Authority and SORN

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

- Title 38, U.S.C., sections 501(a)
- 172VA10/86 FR 72688 VHA Corporate Data Warehouse-VA
- 138VA005Q/74 FR 37093 Veterans Affairs/Department of
- Defense Identity Repository (VADIR)-VA
- 58VA21/22/28 / 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

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?

No, the SORN is not being amended.

The SORN covers cloud usage and storage in the VA Enterprise Cloud (VAEC), which this system is operated within.

4. System Changes

J. Will the completion of this PIA will result in circumstances that require changes to business processes?

Completion of this PIA will not result in circumstances that require changes to business processes.

K. Will the completion of this PIA could potentially result in technology changes?

Completion of this PIA will not result in circumstances that require changes to technology.

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:

1. Description of a disability claim or contention. Generally, this element is not meant to convey PII; however, as it is an open text field value received in the course of retrieving disability claims data from other VA systems, we cannot guarantee PII will not be present; thus ABD-VRO as a rule treats this element as PII.
2. Actor ID of the VA employee who acted on a claim.

PII Mapping of Components (Servers/Database)

Automated Benefits Delivery - Virtual Regional Office (ABD-VRO) consists of 1 key component (database). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Automated Benefits Delivery - Virtual Regional Office (ABD-VRO) 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,	Does this system collect PII? (Yes/No)	Does this system	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

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

Application, Software, Application Program Interface (API) etc.) that contains PII/PHI		**store PII? (Yes/No)**			
Internal Amazon RDS database	No	Yes	VA Employee Data stored: • Actor ID of who took the action on the claim. Veteran Data stored: • Free form text field containing a description of a disability claim or contention. Generally, this element is not meant to convey PII; however, as it is an open text field value received in the course of retrieving disability claims	These elements are received in the course of retrieving disability claims data from other VA systems. It is stored so that ABD-VRO development teams may have a complete picture of what was retrieved.	Database is running on AWS GovCloud and is encrypted using FIPS 140-2 approved encryption (AES-256). Database access is restricted

			data from other VA systems, we cannot guarantee PII will not be present; thus ABD-VRO as a rule treats this element as PII.		

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?

The sources of information in the system are Benefits Integration Platform (BIP), Benefits Enterprise Platform (BEP), the Benefits Integration Events (BIE) Kafka service, and VA.gov. ABD-VRO does not source information from commercial data aggregators.

VRO no longer sources data from the following systems, but they may be used in future iterations of VRO:

- The Mail Automation System (MAS)
- VistA/CDW
- VA/DoD identity (VADIR)

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.

VA stores disability claim information across multiple systems in the course of processing the claim. ABD-VRO is using these VA-managed sources. ABD-VRO is not using data from a commercial aggregator or data taken from public web sites.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The system creates information – essentially, annotations to a disability claim – and invokes BIP and BEP APIs to store this information in the appropriate VA system of record (the created information is not stored long-term within ABD-VRO).

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?

ABD-VRO uses information provided by other VA systems. The transmission method is through APIs and data streams furnished by those respective systems, in addition to explicit approval by those systems for the VRO use case.

VRO does not collect information directly from individuals.

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.

All data is from VA-managed sources, each with their own safeguards. VRO does not additionally check data from these sources for accuracy; it would be difficult to find an appropriate resource to cross-reference data. To ensure the integrity of the data during transmission, ABD-VRO uses secure transport protocols and rotates its certificate/token credentials.

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?

The system does not access 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

VRO is a system supporting the VBA Automated Benefits Delivery initiatives and is sponsored and managed by the Office of the Chief Technology Officer (OCTO). VRO collects information from other systems as specified in the SORN stated in 3H and listed below.

- The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.
- 172VA10/86 FR 72688 VHA Corporate Data Warehouse-VA
- 138VA005Q/74 FR 37093 Veterans Affairs/Department of
- Defense Identity Repository (VADIR)-VA
- 58VA21/22/2886 FR 6158 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

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:

The privacy risk is that control of an individual's PII could be lost, exposing it to parties that could use it for fraudulent purposes or to commit harm to the individual. The data elements needed for VRO are those that would enable a user to verify the identity of the individual who had submitted the benefit claim. These same data elements could be used to commit identify fraud.

Mitigation:

- Data is protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. Access to the data is restricted; those with access are explicitly approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance is enforced for all staff maintaining the VRO system.

- The system is not a system of record for any of the data it stores; loss of the system data would not disrupt processing of beneficiary claims. When the system communicates with other APIs about a Veteran's materials, proxy claim ID or participant ID is used, rather than the Veteran's integrated control number (ICN) or SSN. Furthermore, neither ICN nor SSN data are stored in ABD-VRO.

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.

- Provides teams with data insights into the claims process so they can quickly validate their assumptions and improve the overall claims process
- Allows teams to quickly stand-up applications on the platform so that they can use this data to build custom applications that improve the overall claims process

PII/PHI Data Element	Internal Use	External Use
Description of claim or contention (free form text field that cannot be guaranteed to be free of PII; thus, we treat it as a PII data element)	This element is included as part of retrieving disability claims data from other VA systems and provides greater context on the nature of a claim or contention, which may inform how it's processed.	Not used
Actor ID of the VA employee who acted on a claim	This element is included as part of retrieving disability claims data from other VA systems and provides greater context on the nature of a claim or contention, which may inform how it's processed.	Not used

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?

VRO does not conduct data analysis of this nature.

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.

VRO applications analyze claims submitted on VA.gov and can take certain actions, depending on the claim. For disability claims, the Contention Classifier takes the Veteran's disability contention and matches with the appropriate contention code internally used by VA. VRO is also able to merge the multiple EPs that result when a Veteran files multiple disability claims. If the claims are eligible for merging, VRO uses an API provided by BIP to merge the EPs into a single claim, which updates the claim(s) in VBMS. In these cases, the VRO-produced information is applied to existing records; and do not warrant action being taken.

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?

Data is secured in transit by use of secure transport protocols (secure hypertext transport protocol, https). Veteran disability form data is stored at rest using FIPS 140-2 compliant encryption.

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

The system is not collecting, processing, nor retaining Social Security Numbers.

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

All PII/PHI is secured in transit and stored at rest using FIPS 140-2 compliant encryption. Access to PII/PHI is restricted, and all individuals of tenant teams complete Privacy and HIPAA Training.

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?

VRO access will be limited to users who already have access to PII to perform their job duties.

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

Employees will have taken the proper VA training.

2.4c Does access require manager approval?

Access to PII for any enhancement must be approved through the VRO intake process.

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

VRO does not explicitly monitor, track, or record access to PII. System logs provide an audit trail of when VRO requests disability claim information - which might include PII - from other VA systems and stores a local copy.

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

The VRO Team is responsible for assuring the safeguards of the PII.

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*

A description of individual disability claims and contentions is the only potential PII that is retained by the system.

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.*

VRO does not permanently store data nor create files that would need to be archived. It may store some VA generated form data as part of temporary storage for analysis, which would be considered out of scope for NARA archival but in any case, this data would be purged when analysis is completed.

The information is retained following the policies and schedules of VA's Records management Service and NARA in VBA Records Control Schedule, VB-1, Part I and VBA Records Control Schedule, VB-1, Part II.

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?

VRO does not retain information, however, source systems comply with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500 in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). VRO does not retain information, however, source systems records are retained according to VBA Records Control Schedule, VB-1, Part I and VBA Records Control Schedule, VB-1, Part II.

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

Not applicable, as VRO does not create records of this nature.

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.

The system stores data in an online database in the VA Enterprise Cloud (VAEC). As noted in previous responses, this data does not need to be transferred to NARA. It is destroyed via deletion from the database, in accordance with VAEC best practices and the VA Directive 6500 VA Cybersecurity Program.

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.

VRO testing in development and user acceptance testing (UAT) environments use simulated Veteran records. Only testing in a prod-test environment may contain PII. Testing in the pre-prod environment will be limited to select test cases to ensure that the end-to-end workflow is correct. Access to run the tests is limited to select users who have completed HIPAA training and will follow appropriate practices for data privacy.

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:

The risk to privacy may occur due to unauthorized access of the information used by VRO and retained by the source systems.

Mitigation:

Access is limited to select users who have completed HIPAA training and will follow appropriate practices for data privacy.

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***
VA.gov	VRO shares the maximum disability rating for disability conditions. This information is displayed to users submitting a claim on VA.gov. A user logged in to VA.gov might see information that is received from VRO.	VRO stores a description of the claim (as fetched from BIP). This field might contain PII.	FIPS 140-2 compliant encryption (HTTPS)
Business Integration Platform (BIP) API	BIP provides APIs to allow for getting information on a claim; setting status on a specific claim; and routing claims.	A description of the claim is present when VRO receives claim information from BIP API, and the description field might contain PII.	Point to Point - HyperText Transfer Protocol Secure (HTTPS)
Business Integration Events (BIE) Kafka	Receive processing status change notifications for the 526 (disability compensation) form.	A description of the claim might be included in the information VRO receives from BIE Kafka, and the description field might contain PII. BIE Kafka also includes the actor ID of the	Transmission Control Protocol

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*
		employee who took action on the claim.	
Benefits Enterprise Platform (BEP)	Annotate a claim with the identifier of an associated claim stored in VBMS.	Does not involve PII/PHI.	Point to Point - HyperText Transfer Protocol Secure (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 is that a loss of control of PII during internal sharing and disclosure could occur if the information is not encrypted and if the information is not limited to authorized users.

Mitigation:

The data retrieved for validation and aggregation in VRO are encrypted during transit and at rest. VRO access is limited to users who are already authorized to view PII in order to perform their job duties.

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 System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***

none				

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:

There is no external sharing.
Mitigation:

There is no external sharing.

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.

This system does not collect information from an individual. VRO relies on information that has been collected by the Department or was provided by the Veteran as part of the disability claim submission process. The source systems that transmit data to VRO provide notice regarding collection of information.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

The source systems that transmit data to VRO provide notice regarding collection of information.

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 source systems (such as VA.gov) provide notice to individuals regarding appropriate use of their data because those systems are the point of collection and maintenance of the individual's data.

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.

VRO processes existing information that has been collected by the Department or was provided by the Veteran as part of the disability claim submission process. Individuals

have the opportunity and right to decline to provide information to these source systems. In such cases, the individual is not penalized nor denied service by the VRO system.

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.

VRO relies on the source systems (VA.gov) to provide and manage consent to particular uses of information.

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:

This is not applicable to VRO.

Mitigation:

VRO relies on the notice to individuals that is provided by source systems (VA.gov). See the Privacy Impact Assessment for VETERANS-FACING SERVICES PLATFORM VA.GOV (VFSP-VA.gov), section 6.4 for additional information.

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.***

The system processes information submitted via VA.gov, which has a dedicated public webpage with resources for Privacy Act Requests, to allow individuals to gain access to their own personal records. The webpage is located at https://department.va.gov/privacy/privacy-act-requests/ .

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)?

VRO is not exempt from the access provisions of 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?

VRO is a Privacy Act system covered by the SORN:

- 58VA21/22/2886 FR 6158 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

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.

Since VRO data is fetched from other VA systems that are considered systems of record, and VRO itself is not a system of record, VRO does not have procedures for correcting inaccurate or erroneous information. Incorrect information would need to be corrected within the respective source system.

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.

Not applicable, as VRO does not add or change veteran data. If an individual believes that information is incorrect, they will address that to the source system. Additionally, the veteran can follow the redress described in 7.4.

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.

An individual may appeal a decision if the individual believes there was inaccurate information within their records. The individual can request updates to their information via the source systems that provide the data to VRO.

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:

The privacy risk is that an individual's PII is incorrect and that there is not a process for the individual to have the information corrected. Incorrect information could lead to an adverse outcome in the claim adjudication process, which is one reason an individual would want to correct the PII.

Mitigation:

VRO is not a source of PII that is being processed on behalf of the individual in the benefit adjudication process. There is no mechanism possible for an individual to change the data within VRO. However, an individual would be able to request that the source system perform a change. That process would be implemented by the source system. Subsequent requests from VRO to the source system would utilize the updated information. Thus, the need for information to be corrected or amended is addressed at the source systems.

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?

VRO permits access only to other established VA systems after performing an intake of the use case. VRO does not grant access to individual users.

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 other agencies will not access 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.

VRO is a middleware application that other VA systems access programmatically, through a VRO API. The VA systems use the VRO API to perform functions related to processing disability claims, however the VRO API does not change the information submitted by the Veteran in their disability application, and in this sense might be considered read-only access to the Veteran-supplied information.

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.

VA contractors have access to the system and the PII. Their involvement is primarily to refine features of the system and improve system stability. Contractors for this system

complete an onboarding process developed by OCTO, HIPAA training, and will follow appropriate practices for data privacy.

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.

VA Privacy and HIPAA Training is required for users of the system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* **Approved**
2. *The System Security Plan Status Date:* **October 11, 2022**
3. *The Authorization Status:* **Approved**
4. *The Authorization Date:* **October 11, 2022**
5. *The Authorization Termination Date:* **Continuous**
6. *The Risk Review Completion Date:* **December 08, 2022**
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)*

Yes, the system uses Amazon Web Services (AWS) within the VA Enterprise Cloud (VAEC). The system is deployed as a tenant of VA's Lighthouse Delivery Infrastructure (LHDI) and falls under LHDI's ATO.

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.*

(System utilizes VAEC.)

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.

(System utilizes VAEC.)

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.

(System utilizes VAEC.)

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).

(System utilizes VAEC.)

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

ID	Privacy Controls
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.

LAKISHA WRIGHT

Digitally signed by LAKISHA WRIGHT
Date: 2024.08.08 14:25:25 -04'00'

Privacy Officer, Lakisha Wright

JEFFREY GARDINER

Digitally signed by JEFFREY GARDINER
Date: 2024.08.08 12:26:18 -04'00'

Information System Security Officer, Jeffery Gardiner

EMILY THEIS

Digitally signed by EMILY THEIS
Date: 2024.08.08 11:05:37 -05'00'

Information System Owner, Emily Theis

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).

172VA10/86 FR 72688 VHA Corporate Data Warehouse-VA

138VA005Q/74 FR 37093 Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA

58VA21/22/2886 FR 6158 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

https://www.oprm.va.gov/docs/SORN/Current_SORN_List_01_10_2023.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