Privacy Impact Assessment for the VA IT

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

Veterans Benefits Administration (VBA)

Chief Technology Officer (OIT-005E)

Date PIA submitted for review:

5/1/2023

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)	Andrew Vilailack	*andrew.vilailack@va.gov*	*(813) 970-7568*
Information System Owner	*Zachary Goldfine*	*Zachary.Goldfine@va.gov*	*(202) 756-9088*

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

The Virtual Regional Office Platform (VRO) provides capabilities to fast-tracks Veterans' disability claims. It is a custom-developed platform and capabilities owned by VBA that leverages VHA computable medical data to automate decision-less administrative steps in the disability claim adjudication process. There are a few core features of VRO:

1. Analyze incoming claims for fast-track and automation eligibility.
2. VRO allows for the temporary storage of veteran information as required for claims analysis. Data is encrypted in transit and at rest using FIPS 140-2 approved encryption, access controls are in place to limit access to required parties.

Veteran PII and PHI flows through the VRO, between various VA systems such as the VHA's Corporate Data Warehouse (CDW), VA/DoD identity (VADIR) and VBA's Veterans Benefits Management System (VBMS), its eFolder, as well as VA.gov disability benefit transaction data.

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. The IT system name and the name of the program office that owns the IT system.
The system is called the Virtual Regional Office (VRO), built and maintained by the Office of the CTO in partnership with VBA as the key business stakeholder.

B. 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. Indicate the ownership or control of the IT system or project.
The VRO system will be deployed as a minor app within the Lighthouse Delivery Infrastructure (LHDI) platform owned by OIT. It will be maintained under the control of the Office of the CTO.

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

VRO aggregates data from VA systems and provides the information in a format that helps benefits claim adjudicator with data review and data entry. VRO is not a public-facing system, but rather an automation tool that will improve manual processes.

Information about individual Veterans is stored in a few types of data stores. All PII or confidential information is kept only long enough to process the claim or to analyze the data such as training machine learning models. All PII or confidential data is stored using FIPS 140-2 compliant encryption.

E. A general description of the information in the IT system and the purpose for collecting this information.

The system operates as middleware providing data where needed on an ad hoc basis. It does not create individual data. It handles and stores Veterans Claims related data sourced from other VA systems such as Lighthouse Health API's, BGS, as well as VA.gov sourced data.

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

The VRO system makes data related to Veteran's health and service history available to other systems that are used in the disability benefit claim process. The VRO system is built on the Lighthouse DI system to provide data via API endpoints to other systems within the VA network. VRO retrieves data from Lighthouse APIs such as the Health Data API.

The VRO will also house VA.gov originated benefits forms related data of which the veteran can enter health or PII. This for data will be used to develop machine learning models to allow the platform to automate claims.

G. Whether 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. A 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,
- 58VA21/22/2886 FR 6158 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.

D. System Changes

J. *Whether 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. *Whether 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.

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*
☐ 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)

Also:
Disability Benefit Claim
Current Disability Benefit Record
Data collected from the VBA-21-526EZ from, APPLICATION FOR DISABILITY COMPENSATION AND RELATED COMPENSATION BENEFITS. This could include PII in free form fields that are not labeled to hold PHI/PII.

PII Mapping of Components (Servers/Database)

<**Information System Name**> consists of <**number**> key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by <**Information System Name**> 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	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
N/A	N/A	N/A	N/A	N/A	N/A

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?

VRO will not directly connect to any external database systems, but rather will rely on data transferred via API calls. All data is sourced from existing VA data systems including the Mail Automation System (MAS) and Lighthouse APIs (which sources data from VistA/CDW). VA/DoD identity (VADIR) and VBA's Veterans Benefits Management System (VBMS).

VRO will allow for VA.gov generated form data to be uploaded directly to approved datastores on the platform.

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.

The goal of VRO is to reduce time for decision making by using data that has already been captured within VA systems. All data is sourced from other VA systems (such as VistA/CDW data via Lighthouse Health API), VA-authorized systems (such as the Mail Automation System) or VA.gov

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

Mail Automation System (MAS), Lighthouse, VA.gov, VBA

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?

VRO does not directly collect data from individuals, but instead is downstream from the initiation of a disability benefit claim. The Veteran will submit a claim via the Mail Automation

System (MAS) or the VA.gov web site. VRO will collect additional data (i.e., personal data, medical history, service history, and financial history) that already exists in VA data stores through use of secure API calls.

VRO will house VA.gov sourced benefit form information to develop and train ML model as well as other analysis.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give 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 sources, so VRO will rely on those sources for accuracy. This data cannot be verified against any other sources. For example, VRO calls the Lighthouse Patient Health API to retrieve medical history. That API itself connects to the Corporate Data Warehouse (CDW) for data. VRO trusts that the source system (CDW) manages data quality. VRO ensures accurate transmission of data via status messages provided by the APIs it calls.

1.4b If the system checks 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:

- The data used in VRO is limited in access. To prevent loss of control and the data retrieved for validation and aggregation uses FIPS compliant encryption for data transfer and storage
- Any APIs that VRO exposes are read-only and do not allow the addition or modification of data retrieved from the Lighthouse API. The APIs require authentication to retrieve information and that authentication is strictly controlled. The users of the PII data currently have access to the VBMS eFolder (that contains PII and PHI for the Veteran) and are authorized to review the PII and PHI of Veterans as part of the adjudication process. These users undergo regular training on the use of the data.

- the system does not present a user-interface; it is a platform that automatically reviews claims and allows for claims data to be analyzed for uses such as machine learning training of models.

- The system using FIPS compliant encryption for data transfer and storage

- The system isn't a system of record for any of the data in the system; if all the data in the system was lost it would not impact beneficiary claims.

- When communication with other APIs, whenever possible the system uses ICN to identify a veteran and SSN is only used when required by a related system.

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 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.

- Internal information usage only
- Provides RVSRs with evidence in a pdf summary sheet to support a rating decision
- Uses the evidence already available within VA systems to prevent lengthy delay while a Veteran would need to wait for a medical exam
- Veterans claims data will be used for claims analysis such as training machine learning models.

Data Elements	Usage
Disability Benefit Claim	ICN and Diagnostic code are the only data elements used to retrieve medical evidence through the Lighthouse API.
Current Disability Benefit Record	May be included on the Veteran summary sheet that is added to the eFolder for review by an RVSR.
Service Record	Used in code to compare service location and time for decision logic.
Social Security Number	Masked SSN may be included on the Veteran summary sheet that is added to the eFolder for review by an RVSR.
Integration Control Number (ICN)	Used to retrieve the Veteran's medical information (medication, observations) associated with a diagnosis code for the applicable period.
Participation ID	May be included on the Veteran summary sheet that is added to the eFolder for review by an RVSR.
Full Name, DOB	Used to compiling the evidence report
Address, Email, Phone	May be included on the Veteran summary sheet that is added to the eFolder for review by an RVSR.
Data collected from the VBA-21-526EZ from, APPLICATION FOR DISABILITY COMPENSATION AND RELATED COMPENSATION BENEFITS. This could include PII in free form fields that are not labeled to hold PHI/PII.	May be used to train machine learning models

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 pulls medical history for a claimed condition and analyzes the data to determine if there is sufficient evidence to route the claim to an RVSR or if additional data is needed. No data is created, but information may be derived and included in a summary report (see 2.2b). The decision logic used within VRO is unique for each specific medical condition that can be claimed under the disability benefits process.

VA.gov form data may be analyzed to understand claims trends, and to train, create, or update a machine learning model.

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 pulls medical history and summarizes it based on filters relevant for a claimed condition. The derived data will be reported in a medical evidence summary sheet in a Portable Document Format (PDF) electronic file. The derived data will be stored in the eFolder file structure within VBMS. Users with access to VBMS will be able to access the derived data via the eFolder.

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?

Social Security Numbers are encrypted in transit and encrypted if stored.. SSN are only used to enable search functions for medical data and only sent if other systems require them.

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

API endpoints exposed by VRO consists of stateless, read-only APIs. HTTPS over SSL/TLS API
All data directly uploaded to the platform is transferred and stored using FIPS 140-2 compliant encryption

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. The user group for this system are the RVSR. Their responsibility is to review the Veteran's claim for disability, compare the claim to medical evidence associated with the Veteran, and then follow regulation in rating the disability. The RVSR has a need-to-know basis for viewing PII in each case. VRO is collecting additional data to include with other files that also have PII for the RVSR to review

Access to veteran disability form data is limited to individuals who have access authorization to access the data. Both contractors and VA staff have taken the appropriate training that is required to view the data.

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

Privacy rules applicable to the RVSR's usage of the information provided by VRO is documented as part of the RVSR role. VRO does not change access requirements.

Access to veteran disability form data is to individuals who have authorization. Both contractors and VA staff have taken the appropriate training that is required to view the data as part of their onboarding process.

2.4c Does access require manager approval?

RVSRs will access the data that VRO supplies as approved by their manager.
Stored Veteran claims data does not require any special authorization. Both contractors and VA staff have taken the appropriate training that is required to view the data.

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

VRO does not change the access methods to the data. RVSRs may be monitored in their usage of the VBMS system and eFolder which is outside the control of VRO.

Access to veteran disability form data that is stored for machine learning training does not require any special authorization. Both contractors and VA staff have taken the appropriate training that is required to view the data.

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

RVSRs will continue to be responsible to safeguard PII that is available for their usage within VMBS and eFolder.
VA form generated data will that is stored on the platform will be safeguarded by the team that uploads the data for processing and analysis.

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

Any PII retained for machine learning and training will be removed after the modeling and training is complete. All claims' data is transferred and stored using FIPS 140-2 compliant encryption

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 from data as part of temporary storage for analysis (such as training machine learning models), but the data will be purged as soon as the 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 II & VBA Records Control Schedule, VB-1, Part I.

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 II & VBA Records Control Schedule, VB-1, Part I.

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

The system will not retain records are retained according to VBA Records Control Schedule, VB-1, Part II & VBA Records Control Schedule, VB-1, Part I.

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.

Most records within VRO are electronic records that are not persisted on disk subsystems. The records are temporary in the system's memory and will be released upon system shut down. Therefore, no file destruction is required. The one exception is that, VRO may retain veteran disability claim form data for the purposes of analysis or training ML models, and in that case as well as source systems that the VRO will share SPI from will adhere to VA directives to the procedure for the elimination or transfer of SPI as follows:

"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. https://www.va.gov/vapubs/search_action.cfm?dType=1

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 just a few test cases to ensure that the end-to-end workflow is correct. Access to run the tests is limited to just a few users who have completed HIPAA training and will follow appropriate practices for data privacy.

Accessing Veteran disability form data will be limited to VRO team members, who have completed required VA Privacy training and will follow appropriate practices for data privacy.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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. VRO does not retain the information collected and the data is available for a minimum amount of time, until a timeout (~60 seconds) is reached, then data is released from memory.

In terms of veteran disability form generated data, the PII will only be maintained on the system as long as necessary to do analysis or train ML models. Only the data subset that is necessary to train the ML models will be stored on the system.

Mitigation:
Due to the short storage time for data, the mitigation approach is to secure the data via encryption and access authentication for the short duration that the data is available to the requesting system.

In terms of veteran disability form generated data, the PII will only be maintained on the system if necessary to do analysis such as training Machine learning models, the data will be stored in a VA approved encrypted and compliant method.

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***
CTO Office (Product Engineering)	Veteran medical evidence needed to compile for rapid ready decision and for presentation to RVSR (Rating Veteran Service Representative)	Medical Record, Current Disability Record, Disability Benefit Claim Record, Social Security Number	Point to Point - HyperText Transfer Protocol Secure (https)
Business Integration Platform (BIP) API	BIP provides APIs to allow for setting status on a specific claim to support claim routing as well as a service to provide uploading of a document to the eFolder.	Medical Record, Current Disability Record, Disability Benefit Claim Record, Social Security Number, Integrated Control Number, Participant ID, Full Name, DOB	Point to Point - HyperText Transfer Protocol Secure (https)
VHA's Corporate Data Warehouse (CDW)	CDW is a business-driven information repository that retains information that is integrated, consistent, detailed, historical, and valuable in decision	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number, Fax Number, email Address, Race/ethnicity, Member's maiden name, Current medication, Previous	VA OIT required security controls; user access authorizations managed through a centralized process; project membership

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*
	making for key Stakeholders. The data warehouse is an enterprise asset encompassing multiple subject areas and including departments and lines of business.	medical records, Medical Record Number	restricted to minimum necessary
VA/DoD identity (VADIR)	VADIR is a repository of military personnel's military history, payroll information and their dependents' data. It is used in conjunction with other applications across VA business lines to provide an electronic consolidated view of comprehensive eligibility and benefits utilization data	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number, Fax Number, email Address, Race/ethnicity, Member's maiden name, alias, family relations, service information, education, benefit information, association to dependents, cross reference to other names used, military service participation and status, information (branch of service, rank, enter on duty date, release from active-duty date, military occupations, type of duty, character of service, awards), reason and nature of active duty separation (completion of commitment, disability, hardship, etc.) combat/environmental exposures (combat pay, combat awards, theater location), combat deployments (period of deployment, location/country),	Data transfer and at rest is FIPS 2.0 encrypted. The security for data at rest is Oracle Database Security 19c and in transit is using VA approved transfer methods (e.g.: SFTP, one drive, Teams, HTTPS with TLS, etc.)

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*
		Guard/Reserve activations (period of activation, type of activation), military casualty/disabilities (line of duty death, physical examination board status, serious/very serious injury status, DoD rated disabilities), education benefit participation, eligibility and usage, healthcare benefit periods of eligibility (TRICARE, CHAMPVA), and VA compensation (rating, Dependency and Indemnity Compensation (DIC), award amount).	
VBA's Veterans Benefits Management System (VBMS)	VBMS is an integrated web application intended to streamline Veteran's disability claims process by providing claims processors with an electronic, paperless environment in which to maintain, review, and make rating decisions for veterans' claims. VBMS is a system of systems that interconnects with many local and disparate software components.	Social Security Number, DOB, Medical Records, Disability and Compensation	VA Network only which requires VPN access and 2 Factor Authentication thru the Trusted Internet Connection (TIC) Gateway

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	Allow VRO to train ML models based on VA.gov collected data for the 526 (disability compensation form)	Data collected from the VBA-21-526EZ from, APPLICATION FOR DISABILITY COMPENSATION AND RELATED COMPENSATION BENEFITS. This could include PII in free form fields that are not labeled to hold PHI/PII	FIPS 140-2 compliant encryption (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. Non VRO team members users of the PII data currently have access to the VBMS eFolder (that contains PII and PHI for the Veteran) and are authorized to review the PII and PHI of Veterans as part of the adjudication process. The encryption and access limits will prevent a loss of control of PII data.

VRO team members are authorized VA employees and contractors that have undergone the appropriate training.

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***

IBM - Mail Automation System	Veteran medical evidence needed to compile for rapid ready decision and for presentation to RVSR (Rating Veteran Service Representative)	Medical Record, Current Disability Record, Disability Benefit Claim Record, Social Security Number, Integrated Control Number, Participant ID, Full Name, DOB	172VA10/86 FR 72688, 138VA005Q/74 FR 37093 58VA21/22/2886 FR 6158	Point to Point - HyperText Transfer Protocol Secure (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.

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:
The data that VRO handles contain medical history and service history information. A data breach of this information could lead to reputational damage or financial losses, particularly if the breach results in identity theft.

Mitigation:
VRO does not directly share or disclose data outside the Department.
The data is encrypted in transit and at rest
VRO APIs can only be accessed by authorized applications.

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.

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.

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

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 VistA/CDW) 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. When an individual has opted out of providing information via a source system, the individual will not be penalized or 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 (VistA/CDW/VA.gov) to provide and manage consent to particular uses of information.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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:

<u>Privacy Risk:</u>

The privacy risk is that if sufficient notice is not provided to the individual, then the individual will not be aware of the organization and process for addressing questions around the activities that impact privacy, collection, use, sharing, safeguarding, maintenance and disposal of the individual's PII.

Mitigation:
VRO relies on the notice to individuals that is provided by source systems (VA.gov, VistA, and CDW). If sufficient notice is not provided to individuals, then the organization that manages VRO will discontinue processing of data within VRO until proper notice can be re-established.

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 retrieves existing information from disparate systems across the VA and compiles the information into a summary document for RVSRs to use during the benefit claim adjudication process. The system does not provide a method for the Veteran to view this aggregated data directly.

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:

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

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 only stores information for analysis of data and machine learning. VRO does not have procedures for correcting inaccurate or erroneous information. Incorrect information would need to be corrected within the source system, such as VistA or CDW that are the primary sources for the Lighthouse API information.

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.

VRO is a middleware application between the front-end/veteran facing systems VA.GOV, MAS and the backend datastore (CDW). VRO does not add or change veteran data. If an individual believes that information is incorrect, they would 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 via the Lighthouse API.

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, including VistA and MAS.

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 currently had two use cases:

1. VRO has an API that acts as middleware application between the front-end/veteran facing systems VA.GOV, MAS and the backend datastore (CDW). The VRO permits only approved systems (VA.gov, MAS) to access the APIs using a unique API-key for each API consumer.

2. VRO claims data that is stored for analysis and machine learning is only accessible by authorized VA employees or contractors that have received training to view PHI/PII.

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 does not provide varying access privileges to the data. VRO collects and compiles data to pass to other systems. In the use case that generates a summary report from the data, that document is a read-only file presented to the user.

VRO does allow read write access to the disability claims form data for analysis and machine learning. This data will not be persisted outside the platform and will not update any systems of record with modifications.

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.

Yes, VA contractors that have access to the PII on the platform are authorized to view this information.

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.

The VRO system is a back-end service available only to other systems via authenticated API requests. There are no direct users of VRO, so the only privacy training relevant would be the standard HIPAA training for developers that build systems to handle PII/PHI All individuals that access the system a re required to take VA Annual Rules of Behavior (RoB).

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

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:* **October 11, 2023**
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)*

The system uses AWS within the VAEC.

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.*

N/A

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.

N/A

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.

N/A

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).

N/A

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**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

LAKISHA V WRIGHT 111646

Digitally signed by LAKISHA V WRIGHT 111646
Date: 2023.05.09 11:56:21 -04'00'

Privacy Officer, Lakisha Wright

Digitally signed by ANDREW VILAILACK
Date: 2023.05.09 12:03:52 -04'00'

Information Systems Security Officer, Andrew Vilailack

ZACHARY GOLDFINE

Digitally signed by ZACHARY GOLDFINE
Date: 2023.05.09 10:55:31 -04'00'

Information Systems Owner, Zachary Goldfine

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).

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:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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