Privacy Impact Assessment for the VA IT System called:

Pension Automation

Veterans Benefits Administration

Office of Information Technology

#2062

Date PIA submitted for review:

9/11/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Renu Roy	Renu.roy@va.gov	202 263 9119
Information System Security Officer (ISSO)	Joseph Facciolli	Joseph.Facciolli@va.gov	215-842-2000x2012
Information System Owner	Christina Lawyer	Christina.Lawyer@va.gov	518-210-0581

Abstract

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

Pension Automation (PA) seeks to automate the validation of data and business rules required during each step of the Pension claims workflow to reduce the duplication of effort across claims processing steps and manual processes. Goals of this system include:

- Reducing average days pending for a claim (ADP).
- Increasing the number of claims that can be processed by the current workforce (Throughput).
- Decreasing the inventory of claims pending completion (Inventory).
- Maintaining or increasing processing accuracy (National Accuracy).
- Enabling realignment of Human Resources from Pension claims to process to other critical areas.

• 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?*

Pension Automation is owned by the Office of Information Technology

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

The business purpose of PA is to conduct claim validation processes by performing completeness checks, validating information, and verifying content for VA benefits including business and industry development benefits.

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

PA is owned and operated by the Department of Veterans Affairs (VA).

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?*

The expected number is between 50001 – 75000 and the affected individual is a veteran, spouse, or dependent.

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

Pension Automation interacts with technical interfaces across Veterans Benefits Administration (VBA) to retrieve claim, Veteran, Claimant, and other critical data required to complete the claims process. The primary goal for PA is to run without user interaction, completing the claims process while retaining data integrity across all sub-systems within the Veteran VBA enterprise.

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

PA does not communicate with any external entities outside of VA purview, but processes information internal to the VA. PA conducts information sharing internal to the VA and these connections are discussed in greater detail in section 4 of the PIA.

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?*

PA is hosted on Benefits Integration Platform (BIP). BIP is operated in a single instance of the VA Enterprise Cloud (VAEC) AWS GovCloud, deployed across three Availability Zones.

3. Legal Authority and SORN

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

VA Enterprise Cloud Solutions group partnered with Amazon Web Services (AWS) a FedRAMP provider to offer VA programs the opportunity to host cloud applications. The production environment is hosted in AWS under VA Enterprise Cloud Solutions Office (ECSO) General Support System (GSS) and accredited as FISMA "HIGH" categorization. Custody and ownership of PII and PHI are solely the responsibility of the VA as a tenant of AWS, in accordance with VA policy and NIST 800-144. Both AWS and the VA have a tremendous interest in maintaining security of PII and PHI, including (but not limited to) HIPAA Enforcement Rule of 2006, HIPAA Omnibus, and HITECH. AWS is responsible for physical security, infrastructure security, network and communications for the facility. VA is responsible for the maintaining application, data and system security for the program. VA is the sole owner of all data stored within the system. The contract outlines Management of Security and Privacy Incidents in accordance with VA Handbook 6500.2. Based on determinations of independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages for affected individuals to cover the cost of providing credit protection services to affected individuals. CSPs are required to meet the same requirements when operating on behalf of the federal government.

The System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (July 19, 2012). This SORN can be found at this link, or by searching the VA Privacy Act System of Records Notices (SORN) 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048 5 U.S.C. § 552a, Privacy Act of 1974, As Amended IRS memo FD698-FED-AWS GovCloud-L-031020

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 amendments or revision to SORN is required.

Yes, the SORN does cover cloud usage.

The System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (July 19, 2012). This SORN can be found at this link, or by searching the VA Privacy Act System of Records Notices (SORN) 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048 5 U.S.C. § 552a, Privacy Act of 1974, As Amended IRS memo FD698-FED-AWS GovCloud-L-031020

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 changes to existing business processes.

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

Completion of the PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother’s Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Information
☒ Health Insurance Beneficiary Numbers Account numbers

☒ Certificate/License numbers[1]
☒ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒ Gender
☐ Integrated Control Number (ICN)
☒Military History/Service Connection
☒ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Veteran File Number, Veteran Service Number, Burial Information, Burial letter, development letter, rating code sheet, rating narrative and award letter information, Date of death and associated information on death certificates, Claim Tracked Items, Claim Development Notes, Power of Attorney Information, Veteran Profile, Claimant Profile, Fiduciary Profile, Claim Award Information, Claim Rating Information,

PII Mapping of Components (Servers/Database)

Pension Automation consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Pension Automation and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Camunda	Yes	Yes	• Veteran File Number • Veteran SSN • Veteran First Name	All data collected is required to evaluate pension eligibility so that VA can award the appropriate benefits to	DB uses strong authentication and authorization.

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

			• Veteran Last Name • Claimant File Number • Claimant SSN • Claimant First Name • Claimant Last Name	claimants and dependents.	Only approved user accounts have access. System monitoring and alerts are enabled.
Claim Automator	Yes	Yes	• Veteran Participant ID	Data collected is used for electronic documents and letters sent to the claimant.	DB uses strong authentication and authorization. Only approved user accounts have access. System monitoring and alerts are enabled.

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?

- Benefits Processing Data (BPD) provides extracted data from VA forms and submitted evidence.
- Benefits Gateway Services (BGS) provide veteran and dependent profile information, address information, military service history, development actions, ratings information and award information.
- Veteran Benefits Management System (VBMS) is the primary user interface for VBA users that process Compensation and Pension claims. VBMS provides claim and document-related information.
- DocGen service generates Portable Document Format (PDF) documents after the process has been complete.
- The VBMS eFolder stores electronic documents generated by Pension Automation.
- Package Manager, also known as Centralized Benefits Communication Management (CBCM), provides an interface to distribute packages that are sent through the CBCM vendor for printing and postal mail.

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.
All data collected is required to evaluate pension eligibility so that VA can award the appropriate benefits to Veterans and Claimants.

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

The system does not create information

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?

All information is collected electronically via systems integration.

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?

The 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.

The system evaluates all data through a series of data validation routines and business rule checks as part of the automation process. Various checks are in place to ensure data accuracy. Daily executive reports and operational reports are provided to multiple groups within VA. All decisions are logged and are reviewed when discrepancies are reported. The support team has a well-defined production defect process to resolve issues and research potential issues. Periodic audits by subject matter experts are conducted to review Pension Automation results.

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?

PA does not utilize 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

- PA operates with SORN 58VA21/22/28 located at https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf.

- The VA employee's VBMS identification numbers, the number and kind of actions generated and/or finalized by each such employee, the compilation of cases returned for each employee falls under the authority of the following: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55.

- SSN serves as the Medical Record Number and Unique Identifier for the Veteran. The legal authority is Executive Order 9397, which allows the collection and use of SSN for business purposes/enrollment and 32 CFR 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs.

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: Incorrect data could be sent to Pension Automation when evaluating claims
Mitigation: System controls validate data inputs and there many business rules are executed against the data prior to any decisions. Additionally, there is a full audit trail of system actions

and decision. All data is sourced from trusted VA systems that also have data integrity and privacy controls.

Privacy Risk: Letters sent to incorrect addresses
Mitigation: All addresses are sourced from the VA systems of record, which have data integrity and privacy controls.

Privacy Risk: System is compromised, and data is stolen
Mitigation: The system uses strong security controls. The Department of Veterans Affairs applies consistent security guidance to centralize and standardize account management, network access control, database security, vulnerability scanning and remediation.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Veteran File Number	File Identification purposes	Not used
Veteran Service Number	Used to determine eligibility	Not used
Next of Kin	Used for Veteran's family benefits and correspondence	Not used
Veteran SSN	Used to verify Veteran identity and as a File Number for Veteran	Not used
Veteran First Name	Used to verify Veteran identity	Not used
Veteran Last Name	Used to verify Veteran identity	Not used
Claimant File Number	Used to verify Claimant identity	Not used
Claimant SSN	Used to verify Claimant identity	Not used
Claimant First Name	Used to verify Claimant identity	Not used
Claimant Last Name	Used to verify Claimant identity	Not used
Veteran Profile	Used for update and tracking of related veteran information within the system	Not used
Claimant Profile	Used for claim update, verification, and processing	Not used

Fiduciary Profile	Used for fiduciary correspondence and benefit management with the veteran/beneficiary	Not used
File Number	Used to track and locate file of veteran, claimant, or dependent	Not used
Claim Award Information	Used for claim update, verification, and processing	Not used
Claim Rating Information	Used for claim update, verification, and processing	Not used
Burial Information	Used to determine eligibility	Not used
Military Service History	Used to determine eligibility	Not used
Power of Attorney Information	Used for correspondence and tracking of Power of Attorney information within the claims process	Not used
Claim Tracked Items	Used for claim update, verification, and processing	Not used
Claim Development Notes	Used for claim update, verification, and processing	Not used
Name	Used to verify identity	Not used
Social Security Number	Used to verify identity	Not used
Date of Birth	Used to verify identity	Not used
Personal Mailing Address	Used to send mail to veteran, claimant, and/or dependent	Not used
Personal Phone Number(s)	Used to correspond with the Veteran	Not used
Personal Email Address	Used to correspond with the Veteran	Not used
Emergency Contact Information (Name, Phone Number, etc. of a different individual)	Used to correspond with the Veteran, claimant, dependent, or next of kin	Not used
Certificate/License numbers	Veteran, Claimant, or Dependent tracking	Not used
Vehicle License Plate Number	Veteran, Claimant, or Dependent tracking	Not used
Previous Medical Records	Used to track medical information	Not used
Other Unique Identifying Number	Veteran, Claimant, or Dependent tracking	Not used
Burial letter, development letter, rating code sheet, rating narrative and award letter information	Used to determine eligibility	Not used

Date of death and associated information on death certificates	Used to determine eligibility	Not used
Internet Protocol (IP) Address Numbers	Extracted from VA forms and submitted evidence for claims automation processes	Not used
Financial Information	Used for claim update, verification, and processing	Not used
Health Insurance Beneficiary Numbers	Used to track and manage care relating to Medicare/Medicaid usage of Veteran	Not used
Medications	Used to track medication across medical records and history	Not used
Race/Ethnicity	Extracted data from VA forms and submitted evidence.	Not Used
Gender	Extracted data from VA forms and submitted evidence.	Not Used
Tax Identification Number	Used for Benefit and compensation payments	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?

The system uses a process automation engine to make decisions about the claim. The result is either a pension award denial, grant or "off-ramp," which means the system needs more information. Results are only used for automating the pension claim process.

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.*

The system does not create or make available new or previously unutilized information. It is an automation of the claim decision process.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

All data is encrypted during transit using SSL. Data at rest is only accessible by system administrators and privileged users that are granted access through a standard approval process.

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

All requests require SSL encryption and a JSON Web Token (JWT).

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

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

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?

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

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

Yes

2.4c Does access require manager approval?

Yes

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

Yes

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

The Platform Accelerator teams control the security safeguards that are in all applications that use the BIP framework.

Section 3. Retention of Information

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

3.1 What information is retained?

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

Veteran, Claimant and Dependent information:

- Name
- Social Security Number
- Date of Birth
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Email Address
- Financial Account Information
- Tax Identification Number
- Medical Record Number
- Military Service History
- Other Unique Identifying Number (File Number and Participant ID)
- Date of death and associated information on death certificates

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. **The VA records officer should be consulted early in***

the development process to ensure that appropriate retention and destruction schedules are implemented. *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Data is maintained indefinitely per the below VA data retention policy:

VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII as authorized by NARA: https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

Yes

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

VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII as authorized by NARA: https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

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

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

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

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

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

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

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

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

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

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Benefits Administration (VBMS)	Veteran Benefits Management System (VBMS) is the primary user interface for VBA users that process Compensation and Pension claims. VBMS provides claim and document-related information.	• Veteran File Number • Veteran SSN • Veteran First Name • Veteran Last Name • Claimant File Number • Claimant SSN • Claimant First Name • Claimant Last Name	Receives data via secure SQL Query

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***
Veterans Benefits Administration (BGS)	Benefits Gateway Services (BGS) provide veteran and dependent profile information, address information, military service history, development actions, ratings information and award information.	• Veteran, Claimant, Dependent and Power of Attorney and Fiduciary information • Veteran Profile • Claimant Profile • Fiduciary Profile • File Number • SSN • Claim Award Information • Claim Rating Information Tax Identification Number Financial Information • Burial Information • Military Service History ● Veteran Service Number • Claim Tracked Items • Claim Development Notes • Personal Mailing Address	Receives and updates data via HTTPS /SOAP Request/Response. Secured by SAML and HTTPS.
Veterans Benefits Administration (BIP BPDS API)	Benefits Processing Data (BPD) provides extracted data from VA forms and submitted evidence.	• Veteran, Claimant and Dependent information • 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) ● Next of Kin • Certificate/License numbers • Internet Protocol (IP) Address Numbers • Race/Ethnicity ● Gender • Vehicle License Plate Number • Current Medications	Receives data via HTTPS Request/Response (JSON data format

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***
		• Previous Medical Records • Medical Record Number • Health Insurance Beneficiary Numbers • Other Unique Identifying Number • Date of death and associated information on death certificates	
Veterans Benefits Administration (BIP DocGen API)	DocGen service generates Portable Document Format (PDF) documents after the process has been complete.	• Burial letter, development letter, rating code sheet, rating narrative and award letter information • Veteran Profile • Claimant Profile • Fiduciary Profile • Power of Attorney Information • Personal Mailing Address • File Number	Receives and sends data via HTTPS Request/Response (JSON data format)
Veterans Benefits Administration (BIP Classifier)	The Service-Connected Death Classifier determine if the cause of death meets business criteria for eligibility.	• Date of death and associated information on death certificates	Receives and sends data via HTTPS Request/Response (JSON data format)
Veterans Benefits Administration (VBMS) (eFolder and Package Manager)	The VBMS eFolder stores electronic documents generated by Pension Automation. Package Manager provides an interface to distribute packages for printing and postal mail.	• Burial letter, development letter, rating code sheet, rating narrative and award letter information • Veteran Profile • Claimant Profile • Fiduciary Profile • Power of Attorney Information • Personal Mailing Address • File Number	Receives and updates pdf via HTTPS /SOAP Request/Response. Secured by SAML and HTTPS.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

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

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized by the system. Further, SPI is always encrypted while in transit.

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***
N/A				

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: PA does not share information with systems outside of the VA

Mitigation: PA does not share information with systems outside of the VA

Section 6. Notice

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

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

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

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

Notice was provided under the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (November 8, 2021). This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

"VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA" 58VA21/22/28 (November 8, 2021)

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.

Notice for the collection of Personally Identifiable Information is outlined in SORN 58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

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.

Veterans and Service members may decline or request that their information not be included as part to determine eligibility and entitlement for benefits. No penalty or denial of service is attached with not providing needed information; however, services may be delayed.

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.

While individuals may have the ability to consent to various uses of their information at the VA, they are not required to consent to the use of their information as part to determine eligibility and entitlement for benefits.

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: There is a risk that members of the public may not know that the PA system exists within the Department of Veterans Affairs.

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

Section 7. Access, Redress, and Correction

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

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

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

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

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

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

This system is not exempt from the Privacy Act.

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

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

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

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

VHA Handbook 1605.1 Appendix D ‘Privacy and Release Information’, section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Individuals are notified of procedures for correcting their information via SORN published in the Federal Register (SORN 58VA21/22/286 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA).

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

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

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

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation: By publishing this PIA, and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

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?

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring are performed by the VA's Talent Management System (TMS), the System Owner will then need to review and approve access to the system.

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

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

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

Users must be registered in CSUM (Common Security User Management), a VA internal application. Access to information is based on application user roles for access to the information. For example, Veteran Service employees who need to track the fulfillment of medical information related to a claim for benefits.

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

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

There is a Benefits Integrated Platform (BIP) NDA in place. It covers all personnel working on Pension Automation (PA). The PA development team is comprised of VA personnel and contractors. Access to PA is required for system administrators and developers for day-to-day maintenance of the systems and networks. Review of access to PA is performed on a quarterly basis by the Information System Owner (ISO) and the security engineer. Clearance is required for each person accessing the system. Contracts are reviewed annually by the Contracting Officer's Representative (COR).VA OIT provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems, or VA sensitive information as part of initial training for new users, when required by system changes, and annually thereafter.

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

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

Users are required to complete information system security training activities including annual security awareness training, Privacy training and specific information system security training. The training records are retained for 7 years. This documentation and monitoring are performed using the Talent Management System (TMS).

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

Yes the system was given an Assess Only approval on 11/30/2023

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 11/30/2023
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 11/30/2023
5. *The Authorization Termination Date:* 11/30/2026
6. *The Risk Review Completion Date:* 11/30/2023
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.***

Not Applicable

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, Pension Automation is a Software-as-a-Service system hosted on the Benefits Integration Platform which is hosted in the VA Enterprise Cloud (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.*

<<ADD ANSWER HERE>>

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.

<<ADD ANSWER HERE>>

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**

ID	Privacy Controls
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.

RENU ROY Digitally signed by RENU ROY
Date: 2024.10.21 13:21:58
-04'00'

Privacy Officer, Renu Roy

JOSEPH FACCIOLLI Digitally signed by JOSEPH FACCIOLLI
Date: 2024.10.21 14:03:48
-04'00'

Information System Security Officer, Joseph Facciolli

CHRISTINA LAWYER Digitally signed by CHRISTINA LAWYER
Date: 2024.10.22 08:35:18 -04'00'

Information System Owner, Christina Lawyer

APPENDIX A-6.1

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

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

HELPFUL LINKS:

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

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

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

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

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