Privacy Impact Assessment for the VA IT System called:

VBA Automation Platform

Veterans Benefits Administration

Office of Business Integration (OBI)

eMASS ID #1143

Date PIA submitted for review:

18 December 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	marvis.harvey@va.gov	202-461-8401
Information System Security Officer (ISSO)	Alicia Catney	alicia.catney@va.gov	205-306-6573
Information System Owner	Daniel Hoover	daniel.hoover@va.gov	512-541-0303

Abstract

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

The system, VBA Automation Platform (VBAAP) solution, brings together multiple technologies which work together to read and analyze information, make decisions, and take actions on veterans' claims for compensation. Technical components of VBAAP solution include Robotic Process Automation, Optical Character Recognition engine, Natural Language Processing, Business Intelligence, Business Rules engine, and data Ingestion and Management engine.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

VBA Automation Platform system assists the Veterans Benefits Administration (VBA) with the triage and handling of mail associated with Veterans benefits claims (Veterans' Benefits Mail Automation Service (MAS)), Veterans' Benefits and Claim automation support services such as Veterans disability benefits claims processing (Additional Presumptive Capacity Automation Services (APCAS) Claim Automation, pension claim processing (Pension Optimization Initiative (POI), Private medical records (PMR), National Cemetery Administration (NCA), and Department of Justice (DOJ) Records.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

This is a VA Controlled, non-VA Owned and Operated system. The VBA Automation Platform (VBAAP) IT system/environment is provided by IBM Intelligent Automation Platform (IBM IAP) as a managed service to VA VBA's Office of Business Integration (OBI).

2. Information Collection and Sharing

C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

The number of individuals/veterans the VBAAP system processes is nearly 6,787,884. VA systems acquire data from Veterans. VBAAP acts only as a data processor and the processed data is stored back in the VA systems. Typical clients or affected individuals include veterans, dependents, and VA employees.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

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

The VBA Automation Platform is a managed service that uses unattended automation to assist the Veterans Benefits Administration (VBA) with the triage and handling of mail associated with Veterans benefits claims (Veterans' Benefits Mail Automation Service (MAS)), Veterans disability benefits claims processing (Additional Presumptive Capacity Automation Services (APCAS) Claim Automation) and pension claim processing (Pension Optimization Initiative (POI), Private Medical Records (PMR) retrieval, National Cemetery Administration (NCA), Board of Veterans' Appeals (BVA), DoJ Records Request, and additional approved Benefits Transformation Platform (BTP) Automations. The unattended automation consists of direct system to system integration and robotic process assist (RPA) technology. VBA employees provide the business rules and oversight.

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

The system, VBA Automation Platform (VBAAP) solution, brings together multiple technologies that work together to read and analyze information, make decisions, and take actions on veterans' claims for compensation. Technical components of VBAAP solution include Robotic Process Automation, Optical Character Recognition engine, Natural Language Processing (NLP), AI, Business intelligence, Business Rules engine, data Ingestion and Management engine and so on. VBA employees provide the business rules and oversight needed. The key modules/components of the IBM IAP solution providing VBAAP services are: Robotic Process Automation, Intelligent OCR, AI / NLP, Technologies, Business Process Management, Business Intelligence, and Identity & Access management.

F. *Are the modules/subsystems only applicable if information is shared?*

Listed modules and functions are always applicable and are the core of the service functionality.

G. *Is the system operated in more than one site to include primary and secondary 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 hosted at Amazon Web Services (AWS) GovCloud West location. The system has the capability to migrate to the AWS GovCloud East in case of recovery continuity of operations. Security and privacy controls are maintained consistently in both instances.

3. Legal Authority and System of Record Notices (SORN)

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

The authority for the United States Department of Veterans Affairs (VA) to collect and share data for the purpose outlined under the project scope include:

- Privacy Act of 1974, 5 U.S.C. § 552a, as amended
- Title 10 U.S.C. chapters 106a, 510, 1606 and 1607
- VA Claims Confidentiality Statute, 38 U.S.C § 5701
- Veterans Benefits Title 38, U.S.C. § 501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77.
- Title 5 U.S.C. 5514.

H. *What is the SORN?*

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

I. *SORN revisions/modification*

This system does not require SORN revisions or modifications.

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

This system is not in the process of being modified. The SORN does not require amendment or revision and approval.

4. System Changes

J. *Will the business processes change due to the information collection and sharing?*

☐ Yes
☒ No

K. *Will the technology changes impact information collection and sharing?*

☐ Yes
☒ No

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 Information 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
☒ **Full** Social Security Number
☒ **Partial** 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
☒Sex
☒ Integrated Control Number (ICN)
☒ Military History/Service Connection
☒ Next of Kin
☒ Date of Death
☒ Business Email Address
☒ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (list below)

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

Other PII/PHI data elements: <<Add Additional Information Collected but Not Listed Above Here (For Example, Biometrics)>>

- Cause of Death
- Clinical data
- File Number
- Marital Information
- Packet Id
- Benefits Information
- Email ID

1.2 List 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?

Information is collected from the following sources:

- Veteran Benefits Administration VBMS-Awards and Rating (A&R)
- Veteran Benefits Administration Digitized Mail Handling Services (DMHS)
- Veteran Benefits Management System Web Services eFolder
- Veteran Benefits Administration Benefit Gateway Services (BGS) Web Services
- Master Person Index (MPI)
- Veteran Health Administration Lighthouse Health APIs
- Veteran Benefits Administration Caseflow
- Veteran Benefits Administration Benefits Integration Platform (BIP)
- Veteran Benefits Administration Lighthouse Delivery Infrastructure (LHDI)
- Corporate Data Warehouse (CDW)
- Health Data Repository (HDR)
- Standards and COTS Integration Platform (SCIP)
- Eligibility Office Automation System (EOAS)
- Webpack Web Presidential Memorial Certificate (PMC)
- Private Medical Records (PMR)

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.

Information from sources listed in 1.2a are required for verification of the data received on the intake forms and to automate the processing of claims.

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

The VBA Automation Platform processes veteran's mail and analyzes existing data for presumptive conditions. It does not generate records per the definition of a record by the VA records office and National Archives and Records Administration (NARA). The VBA Automation Platform processes packets in the mail portal and ensures that the correct actions are input into VBMS while also uploading the source documents from the mail portal into Veterans Benefits Management System (VBMS). VBMS is the system of record for benefits information. Pension automation does not generate any additional data beyond mail automation. Presumptive condition uses existing data to evaluate eligibility for presumptive condition. No additional data is generated by any of these systems.

1.3 Methods of information collection

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

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

Information is collected using standard Application Programming Interfaces (API)s and front-end automation leveraging Robotic Process Automation (RPA) technologies.

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?

VBAAP does not retrieve information from forms. VBAAP receives information from other systems via interconnections.

1.4 Information checks for accuracy, and 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 information will be checked using several different methods:

- Using Optical Character Recognition (OCR) /Intelligent Character Recognition (ICR). The confidence level of extraction from each method is evaluated and the results with the highest level of confidence are used.
- Data is validated against VA source systems. If the identifying information does not match, then the data is not processed any further.
- Artificial Intelligence models are used to classify some data elements which cannot be accurately extracted with high level of confidence by the OCR/ICR Process.
- Data which cannot be accurately extracted and validated by the above methods are off ramped for humans to process.

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?

Commercial aggregators are not used.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

The authority for the United States Department of Veterans Affairs (VA) to collect and share data for the purpose outlined under the project scope include:

- Privacy Act of 1974, 5 U.S.C. § 552a, as amended
- VA Claims Confidentiality Statute, 38 U.S.C § 5701
- Title 10 U.S.C. chapters 106a, 510, 1606 and 1607
- Veterans Benefits Title 38, U.S.C. § 501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77
- Title 5 U.S.C. 5514

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

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

<u>Principle of Purpose Specification:</u> The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

<u>Principle of Minimization:</u> The information is directly relevant and necessary to accomplish the specific purposes of the program.

<u>Principle of Individual Participation:</u> The program, to the extent possible and practical, collects information directly from the individual.

<u>Principle of Data Quality and Integrity:</u> VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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:

<u>Privacy Risk:</u> Sensitive Individual Information (SII), Personal Health Information (PHI), and Personally Identifiable Information (PII) data is stored in the system that could be compromised if appropriate safeguards are not in place.

<u>Mitigation:</u> The IBM IAP environment serving VBA Automation Platform is hosted on AWS GovCloud which is a Federal Risk and Authorization Management Program (FedRAMP) High Cloud environment. The VBAAP system adheres to Federal Information Security Management Act (FISMA) Moderate Security & Compliance Authority to Operate (ATO) requirements using VA handbook 6500 and National Institute of Standards and Technology (NIST) SP 800 -53r4 controls.

The implementation of these security standards for data protection enforce role-based access controls, encryption for data in transit and at rest, and continuous monitoring for potential security threats. The VBA Automation Platform incorporates comprehensive audit trails, risk assessments, and incident response mechanisms to maintain high levels of data security and integrity. Specific controls include identity and access management solutions, network security protocols, cryptographic algorithms for data protection, and regular vulnerability scans and penetration testing to ensure ongoing security posture.

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
Name	To establish and process disability, pension, and benefits claims	Not used
Full Social Security Number	To establish and process disability, pension, and benefits claims	Not used
Partial Social Security Number	To establish and process disability, pension, and benefits claims	Not used

Date of Birth	To establish and process disability, pension, and benefits claims	Not used
Personal Mailing Address	To establish and process disability, pension, and benefits claims	Not used
Personal Phone Number(s)	To establish and process disability, pension, and benefits claims	Not used
Personal Fax Number	To establish and process disability, pension, and benefits claims	Not used
Personal Email Address	To establish and process disability, pension, and benefits claims	Not used
Emergency Contact Information (Name, Phone Number, etc. of a different individual)	To establish and process disability, pension, and benefits claims	Not used
Financial Information	To establish and process disability, pension, and benefits claims	Not used
Health Insurance Beneficiary Numbers Account Numbers	To establish and process disability, pension, and benefits claims	Not used
Certificate/License Numbers	To establish and process disability, pension, and benefits claims	Not used
Medications	To establish and process disability, pension, and benefits claims	Not used
Medical Records	To establish and process disability, pension, and benefits claims	Not used
Race/Ethnicity	To establish and process disability, pension, and benefits claims	Not used

Tax Identification Number	To establish and process disability, pension, and benefits claims	Not used
Medical Record Number	To establish and process disability, pension, and benefits claims	Not used
Sex	To establish and process disability, pension, and benefits claims	Not used
Integrated Control Number (ICN)	To establish and process disability, pension, and benefits claims	Not used
Military History/Service Connection	To establish and process disability, pension, and benefits claims	Not used
Next of Kin	To establish and process disability, pension, and benefits claims	Not used
Date of Death	To establish and process disability, pension, and benefits claims	Not used
Business Email Address	To establish and process disability, pension, and benefits claims	Not used
Electronic Data Interchange Personal Identifier (EDIPI)	To establish and process disability, pension, and benefits claims	Not used
Cause of Death	To establish and process disability, pension, and benefits claims	Not used
Clinical Data	To establish and process disability, pension, and benefits claims	Not used
File Number	To establish and process disability, pension, and benefits claims	Not used

Marital Information	To establish and process disability, pension, and benefits claims	Not used
Packet Id	To establish and process disability, pension, and benefits claims	Not used
Benefits Information	To establish and process disability, pension, and benefits claims	Not used
Email ID	To establish and process disability, pension, and benefits claims	Not used

2.2 Describe the types of tools 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?

PII and PHI data associated with claims are analyzed using the following tools and benefit decision are produced and updated on the VA systems. VBAAP analyzes a large amount of unstructured data using Natural Language Understanding/ Processing techniques to make benefit decisions. VBAAP processes data for the purpose of automated routing to claims decision makers and automated claims decision making.

- Robotic Process Automation
- Intelligent OCR
- Business Process Engine
- AI / NLP Technologies
- Business Intelligence

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 VBAAP system/solution adds newly derived information to the claims record which enables the government to make benefit decisions based on available evidence.

2.3 How the information in the system is 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?

Measures in place to protect data in transit and data at rest include – Federal Information Protection Standard (FIPS) 140-2 cryptographic encryption on storage and backups, Transport Layer Security (TLS) on all webservers, and strict access controls and Access Control Lists (ACL).

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Additional safeguards are in place to protect SSNs and minimize the exposure and misuse by implementing strict role-based access controls, multi-factor authentications, and layered security including Virtual Private Network (VPN), private subnets, firewalls, bastion hosts and encryption at all possible levels.

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

In accordance with OMB Memorandum M-06-15, the PII/PHI data in the environment is safeguarded using a multi-layer-security and defense-in-depth approach that include program level adherence to FISMA/FedRAMP controls and security best practices such as role-based access controls, multi- factor authentications, VPN, private subnets, firewalls, bastion hosts and encryption at all possible levels.

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?

All roles/users/administrators of VBA Automation Platform system are vetted through electronic Questionnaires for Investigations Processing (eQIP) clearance process and are required to use VA Personal Identity Verification Card (PIV) smart card to access VA environment. User roles and responsibilities and entitlements are strictly monitored, tracked, and managed by the system owners and the managers. The VBA Automation Platform collects and uses minimum required PII and uses the VA handbook 6500 based FISMA Moderate Risk Management Framework to safeguard the system and the data that is being handled as part of the VBA Automation Platform solution. This is in adherence to the requirements depicted in the contract Performance Work Statement (PWS).

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are they documented, i.e. Policy, SOP, other. And where is this documentation located?

Yes, procedure, controls, and responsibilities regarding PII access are documented in the statement of work and program policy. This documentation is in the primary program document repository.

2.4c Does access require manager approval?

Yes

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

Yes, access to systems containing PII is monitored via system logs collected by the Security Information and Event Management (SIEM) tool.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

The assigned VBAAP system Information System Security Officer (ISSO) and Information System Owner (ISO) are responsible for assuring PII safeguards.

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

The VBA Automation Platform data is not retained beyond 6 months post processing. The list of data elements retained include:

- Name
- Full Social Security Number
- Partial Social Security Number
- Date of Birth
- 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
- Medications
- Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Sex
- Integrated Control Number (ICN)
- Military History/Service Connection
- Next of Kin
- Date of Death
- Business Email Address
- Electronic Data Interchange Personal Identifier (EDIPI)
- Cause of Death
- Clinical data
- File Number
- Marital Information
- Packet Id
- Benefits Information
- Email ID

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

The VBAAP system retains the data during the claims & benefits processing phase for six months. VBAAP discards the data from databases once it is sent to cold storage.

3.3 The retention schedule 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. Please work with the system 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?

While the VBA Automation Platform processes veteran’s mail and analyses existing data for presumptive conditions, it does not generate records per the definition of a record by the VA records office and National Archives and Records Administration (NARA).

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

While the VBA Automation Platform processes veteran's mail and analyses existing data for presumptive conditions, it does not generate records per the definition of a record by the VA records office and NARA. The VBA Automation Platform processes packets in the mail portal and ensures that the correct actions are input into VBMS while also uploading the source documents from the mail portal into VBMS, which is the system of record for benefits information. Pension automation does not generate any additional data beyond mail automation. Presumptive condition uses existing data to evaluate eligibility for presumptive condition. No additional data is generated for any of these systems.

The VBA Automation platform will adhere to General Records Schedule 3.2 (GRS 10, 20, 30) to ensure the security of information technology systems and data, as well as the ability to respond to any computer security incidents that occur.
https://www.archives.gov/files/records-mgmt/grs/grs03-2.pdf

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.

Since all data is stored in the AWS GovCloud storage solution, IBM IAP/VBAAP environment will depend on AWS GovCloud for data handling, retention, and disposal requirements as per the FedRAMP and NIST SP 800-88 compliance guidelines. In general, the VBAAP system will adhere to VA Handbook 6500 and FISMA Moderate controls for all data processing activities. All locally/temporarily stored data during data-processing activities by VBAAP will be purged according to the customer specified timelines by using an automated script which will programmatically delete old data from the tables.

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.

The risk to privacy by using PII data for training is minimized through restricting access to all the VBA Automation Platform environments and associated PII data to only VBAAP staff who hold PIV/HSPD-12 clearance and have a role-based need-to-know. VBA Automation Platform uses data strictly as per the contract/PWS and does not share the PII data with any entities which haven't been approved by the VA. Information is also protected by technical controls including encryption, system segmentation, and role-based access controls.

<u>3.6 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 Privacy Officer (PO) 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: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

Principle of Data Quality and Integrity: *The PIA should describe 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 VBA Automation Platform Veterans processes veteran information which contains PII data. While the data is maintained for no longer than a 6-month period there is a risk associated with maintaining confidentiality and integrity of data retained for any period of time.

Mitigation: All data is stored in the AWS GovCloud storage solution, IBM IAP/VBAAP environment depends on AWS GovCloud for data handling, retention, and disposal requirements as per the FedRAMP and NIST SP 800-88 compliance guidelines. No PII or SPI will be stored in the VBA Automation Platform permanently or greater than six months. Systems storing PII data have in place security monitoring and logging. Additionally preventive security controls include multifactor access controls, encryption at rest, in use and in transit, and role-based access controls.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a VBA Automation Platform consists of 10 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 VBA Automation Platform 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 3.9a 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
Component 1	Yes	Yes	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Information • Health Insurance Beneficiary Numbers Account Numbers • Certificate/License Numbers • Medications • Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Sex • Integrated Control Number (ICN) • Military History/Service Connection • Next of Kin • Date of Death • Business Email Address • Electronic Data Interchange Personal Identifier (EDIPI) • Cause of Death • Clinical data • File Number • Marital Information	Workflow orchestration and temporary storage	NIST SP 800-53 and VA 6500 security controls

			• Packet ID • Benefits Information • Email ID		
Component 2	Yes	No	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Information • Health Insurance Beneficiary Numbers Account Numbers • Certificate/License Numbers • Medications • Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Sex • Integrated Control Number (ICN) • Military History/Service Connection • Next of Kin • Date of Death • Business Email Address • Electronic Data Interchange Personal Identifier (EDIPI) • Cause of Death • Clinical data • File Number • Marital Information • Packet ID • Benefits Information • Email ID	Workflow automation	NIST SP 800-53 and VA 6500 security controls
Component 3	Yes	Yes	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s)	Stores data and audit data for system processing	NIST SP 800-53 and VA 6500 security controls

			• Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Information • Health Insurance Beneficiary Numbers Account Numbers • Certificate/License Numbers • Medications • Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Sex • Integrated Control Number (ICN) • Military History/Service Connection • Next of Kin • Date of Death • Business Email Address • Electronic Data Interchange Personal Identifier (EDIPI) • Cause of Death • Clinical data • File Number • Marital Information • Packet ID • Benefits Information • Email ID		
Component 4	Yes	No	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Information • Health Insurance Beneficiary Numbers Account Numbers • Certificate/License Numbers • Medications • Medical Records • Race/Ethnicity	Automated data analysis	Stateless service, NIST SP 800-53 and VA 6500 security controls

			• Tax Identification Number • Medical Record Number • Sex • Integrated Control Number (ICN) • Military History/Service Connection • Next of Kin • Date of Death • Business Email Address • Electronic Data Interchange Personal Identifier (EDIPI) • Cause of Death • Clinical data • File Number • Marital Information • Packet ID • Benefits Information • Email ID		
Component 5	Yes	No	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Information • Health Insurance Beneficiary Numbers Account Numbers • Certificate/License Numbers • Medications • Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Sex • Integrated Control Number (ICN) • Military History/Service Connection • Next of Kin • Date of Death • Business Email Address	Process automation	NIST SP 800-53 and VA 6500 security controls

			• Electronic Data Interchange Personal Identifier (EDIPI) • Cause of Death • Clinical data • File Number • Marital Information • Packet ID • Benefits Information • Email ID		
Component 6	No	Yes	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Information • Health Insurance Beneficiary Numbers Account Numbers • Certificate/License Numbers • Medications • Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Sex • Integrated Control Number (ICN) • Military History/Service Connection • Next of Kin • Date of Death • Business Email Address • Electronic Data Interchange Personal Identifier (EDIPI) • Cause of Death • Clinical data • File Number • Marital Information • Packet ID • Benefits Information • Email ID	Stores data and audit data for system processing	NIST SP 800-53 and VA 6500 security controls

Component 7	No	Yes	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Information • Health Insurance Beneficiary Numbers Account Numbers • Certificate/License Numbers • Medications • Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Sex • Integrated Control Number (ICN) • Military History/Service Connection • Next of Kin • Date of Death • Business Email Address • Electronic Data Interchange Personal Identifier (EDIPI) • Cause of Death • Clinical data • File Number • Marital Information • Packet ID • Benefits Information • Email ID	Long-term and short-term storage	FedRAMP High AWS cloud security controls
Component 8	No	Yes	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information	Data processing and management	NIST SP 800-53 and VA 6500 security controls

			• Financial Information • Health Insurance Beneficiary Numbers Account Numbers • Certificate/License Numbers • Medications • Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Sex • Integrated Control Number (ICN) • Military History/Service Connection • Next of Kin • Date of Death • Business Email Address • Electronic Data Interchange Personal Identifier (EDIPI) • Cause of Death • Clinical data • File Number • Marital Information • Packet ID • Benefits Information • Email ID		
Component 9	No	Yes	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Information • Health Insurance Beneficiary Numbers Account Numbers • Certificate/License Numbers • Medications • Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Sex	Graphical database management system	NIST SP 800-53 and VA 6500 security controls

			• Integrated Control Number (ICN) • Military History/Service Connection • Next of Kin • Date of Death • Business Email Address • Electronic Data Interchange Personal Identifier (EDIPI) • Cause of Death • Clinical data • File Number • Marital Information • Packet ID • Benefits Information • Email ID		
Component 10	Yes	No	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information • Financial Information • Health Insurance Beneficiary Numbers Account Numbers • Certificate/License Numbers • Medications • Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Sex • Integrated Control Number (ICN) • Military History/Service Connection • Next of Kin • Date of Death • Business Email Address • Electronic Data Interchange Personal Identifier (EDIPI) • Cause of Death • Clinical data	Automated claims and benefits processing	NIST SP 800-53 and VA 6500 security controls

			• File Number • Marital Information • Packet ID • Benefits Information • Email ID		

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Veteran Benefits Administration VBMS-Awards and Rating (A&R)	Update award information	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address	HTTPS, Business Partner Extranet (BPE)

		• Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Financial Information • Health Insurance Beneficiary Numbers Account Numbers • Medications • Medical Records • Race/Ethnicity	
Veteran Benefits Administration Digitized Mail Handling Services (DMHS)	Processes electronic mail packet information towards veterans' Claims & Benefit Processing	• Name • Full/ Partial Social Security Number • Date of Birth • 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 • Medications • Medical Records • Race/Ethnicity	Web Application access over HTTPS Mutual SSL connection
Veteran Benefits Management System Web Services eFolder	Retrieves electronic documents associated with the veteran	• Name • Full/ Partial Social Security Number • Date of Birth • 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 • Medications	Web Application access over HTTPS

		- Medical Records - Race/Ethnicity	
Veteran Benefits Administration Benefit Gateway Services (BGS) Web Services	BGS Web Services	- Name - Full/ Partial Social Security Number - Date of Birth - 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 - Race/Ethnicity	HTTPS, Business Partner Extranet (BPE)
Veterans Administration Master Person Index (MPI)	Veteran data is received to validate the intake	- Name - Full/ Partial Social Security Number - Date of Birth - 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 - Race/Ethnicity	Standard APIs provided by VA, over Site-to-site VPN tunnel
Veterans Health Administration Lighthouse Health APIs	To evaluate presumptive conditions	- Name - Full/ Partial Social Security Number - Date of Birth - Personal Mailing Address - Personal Phone Number(s) - Personal Fax Number - Personal Email Address	REST APIs over BPE

		• Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers Account Numbers • Medications • Medical Records • Race/Ethnicity	
Veterans Health Administration Compensation and Pension Record Interchange (CAPRI)	Functionality to search, view and download of veteran medical records	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers Account Numbers • Financial Information • Medications • Medical Records • Race/Ethnicity	REST APIs over HTTPS
Veterans Administration Enterprise Data Warehouse (EDW)	Data elements for automated claims processing	• Name • Full/ Partial Social Security Number • Date of Birth • 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 • Medications	SFTP

		• Medical Records • Race/Ethnicity	
Veterans Benefits Administration Caseflow	To access past rating decisions and create new	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers Account Numbers • Medical Records	Web Application access over HTTPS
Veterans Benefits Administration Benefits Integration Platform (BIP)	To share extracted and processed claim information	• Name • Full/ Partial Social Security Number • Date of Birth • 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 • Medications • Medical Records • Race/Ethnicity	REST APIs, HTTPS
Veterans Benefits Administration Lighthouse Delivery Infrastructure (LHDI)	Data sharing for automated claims processing	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number	REST APIs

		• Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers Account Numbers • Medical Records • Medications	
Veterans Administration Corporate Data Warehouse (CDW)	Automated Claims Processing	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers Account Numbers • Medical Records • Medications	SFTP
Veterans Benefits Administration Performance, Analytics and Information (PA&I)	To share certain type of claims' extracted information for analysis	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers Account Numbers • Medical Records • Medications	SFTP

Veterans Administration Heath Data Repository (HDR)	To evaluate presumptive conditions	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers Account Numbers • Medical Records • Medications	REST APIs, HTTPS
Veterans Administration Standards and Commercial Off the Shelf (COTS) Integration Platform (SCIP)	Evaluate presumptive conditions, automated claim processing	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers Account Numbers • Medical Records	REST APIs, HTTPS
Veterans Administration Notify	Pre-burial claim processing	• Name • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual)	REST APIs, HTTPS

Eligibility Office Automation System (EOAS)	To process Pre-burial claims	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual)	Web Application access over HTTPS
Webpack Web Presidential Memorial Certificate (PMC)	To process Presidential Memorial Certificate	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual)	Web Application access over HTTPS
Veteran Health Administration Enrollment and Eligibility (EE)	Determine veteran's Enrolment and Eligibility	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers Account Numbers	REST API using HTTPS
Cerner Data Access Service (DAS)	Automated Claims Processing	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number	REST API using HTTPS

		• Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers Account Numbers • Medical Records • Medications	
Pension and Fiduciary (P&F) Service	Data extracted from certain forms	• Name • Personal Mailing Address • Date of Birth • Full/ Partial Social Security Number • File Number • Date of Death • Cause of Death	Standard APIs provided by VA over Business Partner Extranet (BPE)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: The internal sharing of PII is necessary for VBAAP to process veteran information for benefit and claims decision making. There is an inherent risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

Mitigation: Safeguards are implemented to ensure data is not sent to unintended or unauthorized VA organizations. All VA and contract staff attend reoccurring employee security, privacy, and awareness training are required to suspicious activity. Background checks are conducted on VA personnel and their use of data systems includes the use of multifactor authentication, passwords, role-based access controls, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN)s, data encryption are measures utilized within VA facilities and systems. Access to sensitive information and systems is controlled by the VA using least privilege policy. Access must be requested and is only granted based on the individuals need to know and acceptable background check results. Only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted. All VA system with which data is shared maintain security accreditation with VA and federal security policy.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Enterprise Account Validation Service (EAVS) Treasury	Automated claim processing and fraud detection,	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • 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	MOU/ ISA	REST API using HTTPS
Datavant Private Medical Records (PMR)	Retrieves medical records from veteran provided medical providers	• Name • Full Social Security Number • Partial Social Security Number • Date of Birth • Medical Records	Contract	REST APIs/ SFTP
Concord eFax	Sends secure electronic fax to private medical providers.	• Name • Full/ Partial Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Fax Number • Personal Email Address	Contract	REST APIs over SFTP

		- Emergency Contact Information (Name, Phone Number, etc. of a different individual)		

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: The sharing of veteran data by this system is necessary to collect process and validate claims data for individuals to receive benefits. However, there is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: This system has established security controls and audit log review processes to mitigate risks associated through data sharing with authorized external organizations. These controls include a rigorous onboarding process involving VA vetting and periodic validation of system accounts and audits. User access is restricted with role-based access controls and least privilege. Access controls include multifactor authentication, secure passwords, smart Cards. Data connections are encrypted and utilize low trust infrastructure and security controls. Employees are subject to mandatory security and privacy training. System interconnections are monitored and logged. These measures are designed to align with the original data collection's purpose and use, ensuring compatibility during information sharing, while complying with privacy and security controls.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

The VBAAP system does not collect information directly from individuals but from other systems. The privacy notice for this system is included in Appendix A of this PIA. The privacy notice addresses use, disclosure and access acceptable use policy.

6.1b If notice was not provided, explain why.

IBM IAP/VBAAP system does not collect information directly from individuals. These systems which collect data provide a privacy notice to users when they access the system collecting data. When Veterans apply for benefits, The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for benefits.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

The IBM IAP/VBAAP system does not collect information directly from individuals. When Veterans apply for benefits, The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for benefits. Veterans. When Veterans apply for benefits, The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for benefits. The privacy notice for this system is included in Appendix A 6.1 of this PIA.

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.

The IBM IAP/VBAAP system does not collect information directly from individuals. Individuals have the right to decline providing information to the VA systems and personnel. However, failure to provide information may result in denial of access to claims for health care benefits, and various other benefits. Veterans and their family or guardian (spouse, children, parents, grandparents, etc.) cannot decline their information from being included to determine eligibility and entitlement for VA compensation and pension benefits and designate a guardian to manage the VA compensation and pension benefits.

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.

The IBM IAP/VBAAP system does not collect information directly from individuals. For systems which collect information, the Notice of Privacy Practices (NOPP) section "Right to Request Amendment of Health Information" explains how to amend or correct your information. Veterans may request that the VA restrict use or disclosure of all or part of veteran health information. This process is explained in section "Right to Request Restriction" of the NOPP found in Appendix A.

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 Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans Benefits Administration prior to providing the information to the VA.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Policy (NOPP) when Veterans apply for benefits. Additionally, new Notice of Privacy Practices (NOPP) are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records. The NOPP is also available at all VHA medical centers from the facility Privacy Officer. The System of Record Notices (SORNs), NOPP, and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Those wishing to obtain more information about access, redress, and record correction of compensation, pension, education, and vocational rehabilitation and employment records should contact the VA Regional Office as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA.

58VA21/22/28, *Compensation, Pension, Education and Vocational Rehabilitation and Employment Records-VA*
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

The data processed by VBAAP and the systems of record which the VBAAP system sources data for processing are subject to the Privacy Act

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

This system follows applicable Privacy Act procedures and regulations.

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.

Those wishing to access, redress, and correct compensation, pension, education, and vocational rehabilitation and employment records should contact the VA Regional Office as directed in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA.

58VA21/22/28, *Compensation, Pension, Education and Vocational Rehabilitation and Employment Records-VA*
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

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

Individuals are notified of the procedures for correcting their information through the Department of Veterans Affairs Veterans Health Administration NOPP IB 10-163p. Additionally, individuals can refer to SORN 58VA21/22/28 as previously referenced and this PIA which can be found at https://department.va.gov/privacy/privacy-impact-assessments/.

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.

Veterans and other beneficiaries may contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information. Redress information is also contained in the Department of Veterans Affairs Veterans Health Administration NOPP: https://www.va.gov/files/2022-10/10-163p_%28004%29_-Notices_of_Privacy_Practices-_PRINT_ONLY.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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: While this system does not collect information, for the systems which do collect information, there is the risk individuals may seek to access or redress their records held by the VA, not know how to do so, and have their claim processed incorrectly.

Mitigation: Individuals are notified of the procedures for correcting their information through the Department of Veterans Affairs Veterans Health Administration Notice of Privacy Practice, SORN, and this PIA.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

Only the IBM IAP team and the VBA employees assigned to this project are given access to the VBA Automation Platform systems and data after these users are fully vetted through the electronic questionnaires for investigations processing (eQIP) clearance process. The VA contract officer representative (COR), managers/system owners assign, track and monitor every user account, their roles and responsibilities and user life cycle. For every role, Separation of Duties (SoD) and Least Privilege rules are applied to ensure that access to PII is restricted only to those who have a business need to use it.

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?

A small group of DOJ users have access to the DOJ-Record Request web application in the system to support the Camp Lejeune Justice Act of 2022, where in the vetted DOJ users are provided access to electronic records of veteran’s identified by VA.

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.

The VA COR, managers/system owners assign, track and monitor every user account, their roles and responsibilities and user life cycle. All user accounts are VBAAP system users and are not traditional end users. For every role, Separation of Duties (SoD) and Least Privilege rules are applied to ensure that access to PII is restricted only to those who have a business need to use it. No regular user accounts are created on this system since this system provides only the robotic processing automation (no human intervention) for the Benefits and other processes and workflows.

8.2a. Will VA contractors have access to the system and the PII?

Yes, contractors will have access to design and maintenance of VBAAP. The contractors are under contract for this work and under non-disclosure agreement as well as other contract specific non-disclosure agreement.

8.2b. What involvement will contractors have with the design and maintenance of the system?

IBM IAP, the managed services provider for VA's VBA Automation Platform, ensures that there are NDAs/BAAs in place with any Third-Party contracting organizations that are part of the overall VBAP systems and solution. IBM IAP/VBAAP system is hosted on AWS GovCloud and that CSP account governs the vendor risk management processes. IBM and VA have a PWS and ISA-MOU in place.

8.2c. Does the contractor have a signed confidentiality agreement?

Confidentiality is addressed under the contractor statement of work. Confidentiality Rules of Behavior are addressed annually under VA Privacy and Information Security Awareness and Rule of Behavior.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

Yes, the contractor has an implemented Business Associate Agreement for applicable PHI.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?

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.

Non-disclosure is addressed under the contractor statement of work. Non-disclosure Rules of Behavior (RoB) are addressed annually under VA Privacy and Information Security Awareness and RoB. This training and agreement are updated annually by the Program Management Office (PMO).

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

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

VA 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. All users of the VBA Automation Platform are provided the VA Privacy Information Security (PISA) training and VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. Additional trainings and role-based trainings may also get assigned based on role of a user. Annual recertification is required for all trainings.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 11/4/2024
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 2/25/2024
5. *The Authorization Termination Date:* 2/24/2025
6. *The Risk Review Completion Date:* December 2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

Yes, the IBM IAP/VBAAP system uses Cloud technology and is hosted on AWS GovCloud. The AWS GovCloud Cloud services provider (CSP) has a FedRAMP agency authorization and the VBAAP Managed Services has FISMA Moderate agency ATO that adheres to NIST and VA Handbook 6500 controls. The AWS GovCloud is an IaaS model while the IBM IAP managed service is a PaaS and SaaS model.

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

CSP AWS GovCloud – FedRamp High, FedRAMP, IBM-VA Automation Platform Package ID: F1603047866

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.

Yes, AWS GovCloud, as a CSP has access and ownership to ancillary data.

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.

AWS is a CSP. AWS GovCloud provides details about the CSP responsibility matrix, data collected and controls information. The CSP contract/account abides with FedRAMP High security, privacy, compliance and accountability requirements as a condition to maintain their FedRAMP High certification. As a business owner of the data that is hosted in this environment, VA has the ultimate responsibility and accountability towards safeguarding veterans' data.

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).

Yes, the IBM IAP/VBAAP is utilizing Robotic Process Automation (RPA) tools to automate VBA processes by integrating with VA systems.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

MARVIS HARVEY Digitally signed by MARVIS HARVEY
Date: 2025.04.14 13:24:10 -05'00'

Privacy Officer, Marvis Harvey

ALICIA CATNEY Digitally signed by ALICIA CATNEY
Date: 2025.04.14 15:54:52 -05'00'

Information System Security Officer, Alicia Catney

DANIEL HOOVER Digitally signed by DANIEL HOOVER
Date: 2025.04.14 12:09:21 -05'00'

Information System Owner, Daniel Hoover

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).

Privacy Notice: "This U.S government system is intended to be used by [authorized VA network users] for viewing and retrieving information only, except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA. All use is considered to be with an understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms.

Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties."

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

Notice of Privacy Practice (NOPP): When Veterans apply for benefits, The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for benefits. A signed statement acknowledging that the individual read and understood the NOPP. https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

VA Privacy Impact Assessment (PIA) library: Privacy Impact Assessments (PIA) - Privacy

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)