Privacy Impact Assessment for the VA IT System called:

VBMS-Fiduciary

Veterans Benefits Administration

Office of Information and Technology

eMASS ID #2044

Date PIA submitted for review:

05/08/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.harvey@va.gov	314-964-5469
Information System Security Officer (ISSO)	Thomas Wolf	Thomas.Wolf5@va.gov	512-529-8325
Information System Owner	Christina Lawyer	Christina.lawyer@va.gov	518-210-0581

Abstract

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

The VBMS-Fiduciary application is integrated within the Veterans Benefits Management System (VBMS) to enable the Fiduciary Program to expedite qualification, appointments of fiduciaries, and release withheld VA funds to beneficiaries. It will also provide a more effective means for VA to meet its mission of oversight and protection of our Veterans and their survivors. Utilization of more enhanced and modern technology will allow for an increase in the timeliness of fiduciary appointments, reduction of accounting disapproval rates, and enhance the ability to manage workload, oversight, and reporting. VBMS-Fiduciary also allows for increased automation and communication with other applications that are necessary to provide comprehensive functionality to Fiduciary Program customers.

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?*

VBMS-Fiduciary's purpose is to modernize and expedite the process surrounding fiduciaries and through the use of enhanced technology, allow for increased automation and communication with other applications to increase functionality to Fiduciary Program customers.

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.*

VBMS-Fiduciary is owned and operated by the VA.

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 VBMS-Fiduciary application manages over 470,000 fiduciary and 450,000 beneficiary records across the following Fiduciary Hubs:
- VACO (Station 101)
- Columbia, SC (Station 319)
- Indianapolis, IN (Station 326)
- Louisville, KY (Station 327)
- Milwaukee, WI (Station 330)

- Lincoln, NE (Station 334)
- Salt Lake City, UT (Station 341)

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?*

VBMS-Fiduciary is designed, built, operated, and maintained with the requirement to contain records that have Veterans, Fiduciaries and/or Beneficiaries Sensitive Personal Information (SPI) like Name, Social Security Number (SSN), Veteran File Number, Veteran File Number, Birth Date, and Contact Information.

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

VBMS-Fiduciary does not communicate with any external entities outside of VA purview but ingests information internal to the Department of Veteran's Affairs. VBMS-Fiduciary conducts information sharing internal to the Department of Veterans Affairs. Internal sharing discussed in greater detail in Section 4 of this Privacy Impact Assessment (PIA).

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

Yes.

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?*

VBMS-Fiduciary is cloud-based and is not operated in more than one site.

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

H. What is the citation of the legal authority?

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104--- 231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- Privacy Act of 1974; U.S Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 & Title38, US Code section 7301 (a) and Executive Order 9397
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) •
- State Privacy Laws
- The legal authority is 38 U.S.C 7601-7604 and U.S.C 7681-7683 and Executive Order 9397
- 45VA21 – Veterans Assistance Discharge System-VA
- 138VA0005Q - Veterans Affairs Department of Defense Identity Repository (VADIR) - VA
- System of Record Notice (SORN): 58VA21/22/28, VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA (November 8, 2021). This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

I. What is the SORN?

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

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

No amendments or revisions to the SORN are required.

4. System Changes

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

☐ Yes
☒ No
if yes,

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

☐ Yes
☒ No
if yes,

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)

Other PII/PHI data elements: Participant ID, Veteran Patient ID, Benefit Claim, File Number, Medical History

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?

VBMS-Fiduciary system receives information directly from the application's user interface (UI).

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.

VBMS-Fiduciary receives information via data input by the system's end users (VBA fiduciary processers in the Fiduciary Hub Offices) and electronically, via web service calls to Benefits Integration Services (BIS).

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

No

1.3 Methods of information collection

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

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

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?

VBA fiduciary processers in the Fiduciary Hub Offices (Fid Hubs) input information using the VBMS-Fiduciary system web UI. The VBMS-Fiduciary system makes web service calls to other VA-internal systems like BIS to retrieve data.

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

The information is not collected on a form.

1.4 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.

Within VBMS-Fiduciary, Fiduciary Service Representative (FSR) is responsible for ensuring that all information on individual beneficiary records in the Beneficiary Fiduciary Field System is both accurate and current, at the time of any record maintenance or updating.

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?

VBMS-Fiduciary does not utilize a commercial aggregator of information.

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

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048

- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- Privacy Act of 1974; U.S Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 & Title38, US Code section 7301 (a) and Executive Order 9397
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites
- OMB Memo M---99---18, Privacy Policies on Federal Web Sites
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws
- The legal authority is 38 U.S.C 7601-7604 and U.S.C 7681-7683 and Executive Order 939
- System of Record Notice (SORN) 58VA21/22/28 (November 8, 2021)
  Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA
  https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

Principle of Minimization: *The information is directly relevant and necessary to accomplish the specific purposes of the program.*

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

Principle of Data Quality and Integrity: *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:

Privacy Risk: There is risk involved in VBMS-Fiduciary's collection of PII and other sensitive information as required for the application to fulfill its designed purpose.

Mitigation: The information collected is kept to the minimum necessary to complete the applications function and is protected by industry standard security measures on the BIP (Benefits Integration Platform) within VAEC AWS GovCloud environment.

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
Social Security Numbers	Used to verify Veteran identity and as a File Number for Veteran	Not used
Name	Personnel Identification	Not used
Personal Mailing Address	Used to correspond with the individual	Not used
Phone numbers	Used to correspond with the individual	Not used
Personal Email address	Used to correspond with the individual	Not used
Date of birth	Used to verify Veteran identity	Not used
Military service History	Used to determine eligibility	Not used
Financial Account information	Management of compensation/award delivery information to veteran/beneficiary	Not used
File Number	Tracking of evidence and documentation relating to the Veteran with the VA	Not used
Next of Kin	For tracking and updating of benefit information relating to family/dependent	Not used
Medical History	Used to track medical information for eligibility	Not used
Date of Death	Used to determine eligibility	Not used
Participant ID	Linking of information to veteran's file	Not used
Financial information (Routing, Accounting numbers)	Necessary for award and/or compensation delivery to veteran/beneficiary	Not used
Benefit Claim	Used to determine eligibility	Not used

Electronic Data Interchange Personal Identifier (EDIPI)	Used to verify Veteran identity	Not used
Military Branch	Used to determine eligibility	Not used
Veteran Patient ID	Tracking of relevant claim/medical information	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?

VBMS-Fiduciary does not perform any complex analytical tasks, nor does it derive any new data currently.

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

The system does not create or make available new or previously unutilized information.

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?

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

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).

All requests require SSL encryption and a JWT.

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

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

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

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

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

Yes

2.4c Does access require manager approval?

Yes

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

Yes

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

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

Section 3. Retention of Information

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

3.1 What information is retained?

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

In the various sections within the VBMS-Fiduciary application, the following sensitive information is collected, used, disseminated, created, or maintained:

Beneficiary Search: Name, File Number, SSN, Date of Birth, Participant ID, Personal Mailing Address, Military Branch, Military service History

Beneficiary Profile: File Number, Name, SSN, Birth Date, Date of Death, Email Address, Phone Number, Financial information (Routing, Accounting numbers), Personal Mailing Address, Medical History

Fiduciary Search: Name, SSN, Date of Birth, Personal Mailing Address

Fiduciary Profile: Name, SSN, Date of Birth, Personal Email Address, Phone Numbers, File Number, Personal Mailing Address

Field Exam Report: Name, SSN, File Number, Next of Kin

Accounting Audit Tool: Name

Misuse Record: Name

3.2 How long is information retained?

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

Data is maintained indefinitely per the below VA data retention policy: VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII as authorized by NARA: https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

3.3 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?

Yes

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

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

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

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

All paper documentation that is not the property of VA (e.g., DoD-owned documentation) is currently stored by VA after scanning, pending a policy determination as to its final disposition. All documentation being held pursuant to active litigation is held in its native format during the pendency of the litigation. All VBMS eFolders are stored on a secure VA server, pending permanent transfer to NARA where they will be maintained as historical records. Once an electronic record has been transferred into NARA custody, the record will be fully purged and deleted from the VA system in accordance with governing records control schedules using commercial off the shelf (COTS) software designed for the purpose. Once purged, the record will be unavailable on the VA system, and will only be accessible through NARA. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location Version date: October 1, 2023 Page 14 of 31 and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

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

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

VBMS-FID does not use PII for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document in 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: Potential risk of data leak may exist with retaining personal data for any amount of time. Mitigation steps below will reduce this kind of attack surface.

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

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a VBMS-FID consists of 1 key component (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 VBMS-FID 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**
Fiduciary Database	Yes	Yes	Social Security Numbers Names Personal Mailing Addresses Phone numbers Personal Email addresses Next of Kin Medical History Date of Birth Date of Death Veteran Participant ID	Veteran, Fiduciary, and Beneficiary data required to expedite qualification, appointments of fiduciaries, and release withheld VA funds to beneficiaries.	Encryption at rest, encryption in transit using SSL encryption and certificate exchange.

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***
Awards	VBMS-Fiduciary establishes a specific claim type, updates beneficiary diary information, and in certain circumstances, updates or sends correspondence when a specific award is authorized in the Awards system.	File number	Representation State Transfer (REST) web service API (HTTPS)
Benefits Integration Services (BIS)	BIS provides web services that return data not housed in VBMS-Fiduciary, including Veteran data, claim data, etc.	Name File number Social security number Date of birth Participant ID Personal Mailing Address Military branch Date of death	SIMPLE Object Access Protocol (SOAP) over HTTPS using SSL encryption and Certificate exchange

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***
		Personal Email address Telephone Numbers Accounting number Routing number	
Claims API	Claims cover the entire workflow that directs the establishment, development, and processing of a request for benefits covering. A claim is a formal request for benefits that is submitted by a claimant, who could be a Veteran, a dependent of a Veteran, or a person or organization authorized to act on behalf of the Veteran.	Social Security Number Name Personal Mailing Address Benefit Claim	REST web service API (HTTPS)
Docgen	VBMS-Fiduciary uses DocGen via VBMS-Core and VBMS-Fiduciary to generate Fiduciary correspondence.	File number Social security number Date of birth Veteran Patient ID Personal Mailing Address Military branch Name Date of death Personal Email address Telephone numbers Accounting number Routing number	REST web service API (HTTPS)
VEFS Claim Evidence	VBMS-Fiduciary uses Claim Evidence for generated finalized documents and correspondence.	File number	(SOAP) over HTTPS using SSL encryption and Certificate exchange
Package Manager	VBMS-Fiduciary sends Package Manager the document reference ID and the recipient	File number Personal Mailing Address Name	REST web service API (HTTPS)

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***
	information for the printing process.		
Veteran API	VBMS-Fiduciary users Veteran API to retrieve veteran information relevant to the fiduciary, and/or the beneficiary for use within the claim process	File number Name Veteran Patient ID Social Security Number Electronic Data Interchange Personal Identifier (EDIPI)	REST web service API (HTTPS)
Fiduciary Accounting Submission Tool (FASTAPI)	(FAST) is a SalesForce application that provides Fiduciary a portal to submit accounting details for the Beneficiaries they are assigned. FAST also allows for LIEs to review these accountings. The VBMS-Fiduciary application is used by the LIEs to complete the accounting review process.	Name Personal Email Address File Number Veteran Patient ID	REST web service API (HTTPS)
VA Profile	VA Profile supports the synchronization of contact information, as well as other Veteran information domains among VA systems.	Personal Mailing Address	REST web service API (HTTPS)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Section 5. External Sharing/Receiving and Disclosure

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

5.1 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***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing.

Section 6. Notice

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

6.1 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.

VA gathers or creates these records to enable it to administer statutory benefits programs to Veterans, Service Members, Reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran's benefits administered by VA. See the statutory provisions cited in ''Authority for maintenance of the system". This notice is provided by the SORN for better understanding to the reader. The System of Record Notice (SORN) as listed in the Federal Register: 58VA21/22/28, Compensation, Pension, Education, and Rehabilitation Records- VA https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

6.1b If notice was not provided, explain why.

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 The System of Record Notice (SORN) as listed in the Federal Register: 58VA21/22/28, Compensation, Pension, Education, and Rehabilitation Records- VA https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

The Department of Veterans Affairs provides public notice that the system exists in two ways:

1. The System of Record Notice (SORN) as listed in the Federal Register: 58VA21/22/28, Compensation, Pension, Education, and Rehabilitation Records- VA Version date: October 1, 2023 Page 25 of 35 https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

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

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

> Individuals have the right to decline providing information to VA 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 also 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.

> While individuals may have the ability to consent to various uses of their information at the VA, they are not required to consent to the use of their information to determine eligibility and entitlement for VA compensation and pension benefits. The Privacy Act and VA policy require that PII information only be used for the purpose(s) for which it was collected unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information such as use of collected information for marketing.

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

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your 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:

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> 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 individuals may not be aware of what data is being collected or how that data is being used by the VA and/or this application.

Mitigation: The VA mitigates this risk by providing two forms of notice, as identified in Section 6.1, including the System of Record Notice and Privacy Act statement.

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)?

This system is not exempt.

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

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

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

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

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

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

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

> Individuals are notified of procedures for correcting their information via SORN published in the Federal Register (SORN 58VA21/22/286 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA). https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

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

> Procedures for redress and amendment are outlined in the System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records –VA” 58VA21/22/28 (November 8, 2021). This SORN can be

found online at https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your 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: Individuals may seek to access or redress their records held by the VA Office and a risk exists that their claim will not be processed correctly.

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

Section 8. Technical Access and Security

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

Access is requested per VA 6500 policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor, Information System Owner (ISO) and Office of Information and Technology (OIT) approval must be obtained prior to access being granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the Version date: October 1, 2023 Page 29 of 35 system(s) through dual authentication, i.e., a PIV card with a complex password combination (two-factor authentication is enforced). Once inside the system, individuals are authorized to access information on a need-to-know basis.

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

Only VA Employees and Contractors have access to the system.

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

There are End-user, Admin, and Read-only roles for this system.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

The contractors are under contract for this work and under non-disclosure agreement as well as other contract specific non-disclosure agreement.

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

Yes, but only in the production environment.

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

Yes, contractors will have access to design and maintenance of VBMS-FID

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

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

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

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

8.4a If completed, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 10/09/2024
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 12/05/2023
5. *The Authorization Termination Date:* 12/05/2025
6. *The Risk Review Completion Date:* 12/05/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

This system has an Assess Only ATO approval.

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 system is a Software as a Service (SaaS) hosted on Benefits Integration Platform (BIP) which is hosted in the VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) GovCloud.

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.*

The VA maintains ownership of the data, and selects which services can process, store, and host data. The CSP does not access or use the data for any purpose without agreement from the VA. VAEC determines where the data will be stored, including the type of storage and geographic region of that storage. VAEC manages access to its data, and access to services and resources through users, groups, permissions, and credentials that are internally controlled. VAEC chooses the secured state of the data. The CSP provides encryption features that protect data in transit and at rest and provides VAEC with the option to manage their encryption keys. VAEC AWS Enterprise Cloud Capacity Contract - NNG15SD22B VA118-17-F-2284.

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.

The CSPs automatically collect metrics, such as offering usage, occurrences of technical errors, diagnostic reports, settings preferences, backup information, API calls, and other logs. VAEC is the owner of its data (customer data). The CSP does not use customer data and has anonymized metrics to help them measure, support, and improve their services. The CSP has ownership of these anonymized metrics.

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.

Each application in the VAEC is responsible for their data. For all cloud deployment types, the customer owns their data and identities. The customer is responsible for protecting the security of their data and identities, on-premises resources, and the cloud components they control (which varies by service type). This is the Shared Responsibility Model for Security in the Cloud.

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).

VBMS-FID does not utilize Robotics Process Automation at this time.

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

ID	Privacy Controls
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 provided in this Privacy Impact Assessment is true and accurate.

MARVIS HARVEY Digitally signed by MARVIS HARVEY
Date: 2025.06.03 07:00:58 -05'00'

Privacy Officer, Marvis Harvey

THOMAS WOLF on behalf of ISSO as Supervisor
2025.06.02 11:14:20 -05'00'

Information Systems Security Officer, Thomas Wolf

CHRISTINA LAWYER Digitally signed by CHRISTINA LAWYER
Date: 2025.06.02 09:50:58 -04'00'

Information Systems Owner, Christina Lawyer

APPENDIX A-6.1

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

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)