SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.
The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements
under the Federal Information Security Management Act (FISMA).

VA HANDBOOK 6508: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 2014,
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=767&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

VBMS-Fiduciary

Office of Information and Technology (OI&T)

Date PIA submitted for review:

January 11, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	(202) 632-7861
Information System Security Officer (ISSO)	Joseph Facciolli	Joseph.Facciolli@va.gov	(215) 842-2000 x2012
Information System Owner	Gary Dameron	Gary.Dameron2@va.gov	(202) 492-1441

Abstract

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

The purpose of the Department of Veterans Affairs (VA) Fiduciary Program is to protect Veterans and beneficiaries who are unable to manage their VA benefits through the appointment and oversight of a fiduciary.

The VBMS-Fiduciary application will be integrated within the Veterans Benefits Management System (VBMS) to enable the VA 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 will also allow 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 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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? 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.*

- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

The tool Fiduciary used to track data, manage workload, complete work and conduct quality reviews was the Beneficiary Fiduciary Field System (BFFS). The BFFS system is a standalone outdated, labor intensive system which does not allow for accurate oversight and data reporting. The application does not provide field examiners (FEs) the ability to complete cases, attain digital signatures while in the field or utilize mobile/offline technology. The BFFS application limited the ability to automate fiduciary processes, to include workflows and accounting reconciliations. Its inability to seamlessly interface with other VA systems results in duplication of efforts related to data entry, records management and reduces the effectiveness and efficiency of Fiduciary Hub employees. The BFFS system is no longer being used.

The VBMS-Fiduciary application, owned by VA Fiduciary and Pension, will be integrated within the Veterans Benefits Management System (VBMS) to enable the VA Fiduciary and Pension 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 will also allow for increased automation and communication with other applications that are necessary to provide comprehensive functionality to Fiduciary Program customers.

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)

VA Enterprise Cloud Solutions group partnered with Amazon Web Services (AWS) a FedRAMP provider to offer VA programs the opportunity to host cloud applications. The VBMS-Fiduciary application will be deployed onto the Benefits Integrated Platform (BIP) production environment hosted in AWS under VA Enterprise Cloud Solutions Office (ECSO) General Support System (GSS) and accredited as FISMA "HIGH" categorization. Custody and ownership of PII and PHI are solely the responsibility of the VA as a tenant of AWS, in accordance with VA policy and NIST 800-144. Both AWS and the VA have a tremendous interest in maintaining security of PII and PHI, including (but not limited to) HIPAA Enforcement Rule of 2006, HIPAA Omnibus, and HITECH. AWS is responsible for physical security, infrastructure security, network and communications for the facility. VA is responsible for the maintaining application, data and system security for the program. VA is the sole owner of all data stored within the system.

VBMS-Fiduciary operates with SORN 58VA21/22/28 located at located at https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf and Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55. SSN serves as the Medical Record Number and Unique Identifier for the Veteran in this and all VA OI&T Systems. Executive Order 9397, which allows the collection and use for business purposes/enrollment and 32 CFR 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs serves as the highest legal authority for this use.

VBMS-Fiduciary is designed, built, operated, and maintaining 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. As such, the completion of this PIA will not result in any circumstances that could potentially require changes to business practices nor result in technology changes.

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).

VBMS-Fiduciary collects Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system and potential damage to the reputation of the CSP and/or the VA.

Section 1. Characterization of the Information

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

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

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

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

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

☒ Name

☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Other Unique Identifying Number (list below)

Additional SPI: Family Relation, Service Information, Guardian Information, Benefit Information

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, Mailing Address, Military Branch

Beneficiary Profile:
Veteran File Number, Veteran Name, Beneficiary Name, Social Security Number, Birth Date, Date of Death, Date of Incompetency, Email Address, Secondary Email Address, Home Phone Number, Cell Phone Number, Telephone Number 1-4, Accounting Number, Routing Number, Mailing Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country), Physical Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country), Fiduciary Name

Fiduciary Search:
Name, SSN, Date of Birth, Physical Address

Fiduciary Profile:
First Name, Middle Name, Last Name, SSN, Date of Birth, Email Address, Secondary Email Address, Primary Phone, Alternative Phone, Alternative Phone 2, File Number, SSN, Mailing Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country), Physical Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country)

Field Exam Report:
Beneficiary Name, Beneficiary's Social Security Number, Name of Veteran, VA File Number, Veteran's Social Security Number, Fiduciary Name, Name of preferred Fiduciary, Dependent Name

Accounting Audit Tool:
Beneficiary Name, Fiduciary Name

Misuse Record:
Beneficiary Name, Fiduciary Name

PII Mapping of Components

VBMS-Fiduciary consists of one key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VBMS-Fiduciary and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Fiduciary	Yes	Yes	SSN, DOB, Fiduciary and Beneficiary PII	Veteran, Fiduciary, and Beneficiary data required to expedite qualification, appointments of fiduciaries, and release withheld VA funds to beneficiaries.	VA Network only wh requires VPN access Factor Authentication

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

VBMS-Fiduciary system receives information directly from the application's user interface (UI) via data input by the system's end users (VBA fiduciary processers in the Fiduciary Hub Offices) and electronically, via web service calls to Benefit Gateway Services (BGS).

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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 BGS to retrieve data.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.
This question is related to privacy control AP-2, Purpose Specification.

The VBMS-Fiduciary application replaces the legacy Benefit Fiduciary Field System (BFFS) with more enhanced and modern technology to 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.

The electronic presence of Veteran, Fiduciary, and Beneficiary data within the VBMS-Fiduciary system is the result of interaction between connecting systems and directly relate to the program's purpose.

1.5 How will the information be checked for accuracy? How often will it be checked?

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.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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.

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

VBMS-Fiduciary operates with SORN 58VA21/22/28 located at https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf. The VA employee's VBMS identification numbers, the number and kind of actions generated and/or finalized by each such employee, the compilation of cases returned for each employee falls under the authority of the following: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55. SSN serves as the Medical Record Number and Unique Identifier for the Veteran. The legal authority is Executive Order 9397, which allows the collection and use of SSN for business purposes/enrollment and 32 CFR 505.4(a)(b) for individual's rights, benefits, and privileges under federal programs.

1.7 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: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:
Privacy Risk: VBMS-Fiduciary collects Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). This information is specifically collected for the purpose of VBMS-Fiduciary as a system. It is an absolute requirement for the efficacy of VBMS-Fiduciary.

If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and aid the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information specified in section 1.1, the VA can better protect the individual's information.

VBMS-Fiduciary utilizes the existing VBA Common Security System (CSS) that controls user authentication and role-based permissions that VBMS is built on. Permissions are only given after a request and approval of that request by an Information Security Officer (ISO).

Individuals do not have the authority to opt into the VBMS participation but can opt out through a developed and mature process. The amount of information collected is the minimum amount required to make such decisions.

VBMS-Fiduciary provides additional security via to VBA CSS for both integrity and confidentiality which will prevent unauthorized users from gaining access to any data. Additionally, VBMS-Fiduciary is an internally hosted application meaning that only the authorized user can access VBMS-Fiduciary and those users have to be on the VA network which insulates VBMS-Fiduciary from any outside/public access. VBMS-Fiduciary employ a variety of security measures that satisfy controls dictated within the VA 6500 Rev 4 Directive.

Section 2. Uses of the Information

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

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

Identify and list each use (both internal and external to VA) of the information collected or maintained.

This question is related to privacy control AP-2, Purpose Specification.

Full Name: Veteran's identification
DOB: Used to verify Veteran identity
Social Security Number: Used to verify Veteran identity and as a File Number for Veteran
Mailing Address: Used to correspond with the Veteran
Zip Code: Part of the mailing address
Phone Numbers: Used to correspond with the Veteran
Email Address: Used to correspond with the Veteran
Family Relation: Used for Veteran's family benefits
Service Information: Used to determine eligibility
Medical Information: Used to track medical information
Guardian Information: Used to verify if veteran's family member has a guardian
Benefit Information: Used to determine eligibility

In the various sections within the VBMS-Fiduciary application, the following sensitive information is collected, used, disseminated, created, or maintained. The following information is used to search for Beneficiaries and Fiduciaries and to enable the Fiduciary Program to expedite qualification, appointments of fiduciaries, and release withheld VA funds to beneficiaries via the VBMS-Fiduciary application.

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

Beneficiary Profile:
Veteran File Number, Veteran Name, Beneficiary Name, Social Security Number, Birth Date, Date of Death, Date of Incompetency, Email Address, Secondary Email Address, Home Phone Number, Cell Phone Number, Telephone Number 1-4, Accounting Number, Routing Number, Mailing Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country), Physical Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country), Fiduciary Name

Fiduciary Search:
Name, SSN, Date of Birth, Physical Address

Fiduciary Profile:
First Name, Middle Name, Last Name, SSN, Date of Birth, Email Address, Secondary Email Address, Primary Phone, Alternative Phone, Alternative Phone 2, File Number, SSN, Mailing Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country), Physical Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country)

Field Exam Report:
Beneficiary Name, Beneficiary's Social Security Number, Name of Veteran, VA File Number, Veteran's Social Security Number, Fiduciary Name, Name of preferred Fiduciary, Dependent Name

Accounting Audit Tool:
Beneficiary Name, Fiduciary Name

Misuse Record:

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

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

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

Add answer here:

The 2019 58VA21/22/28 SORN located at https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf defines the information collected from Veterans, use of the information, and how the information is accessed and stored. The information collected is required to expedite qualification, appointments of fiduciaries, and release withheld VAQ funds to beneficiaries. The security controls for the VBMS-Fiduciary application cover 26 security areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; program management; planning; personnel security; risk assessment; systems and services acquisition; security assessment and authorization; system and communications protection; system and information integrity; authority and purpose; accountability, audit, and risk management; data quality and integrity; data minimization and retention; individual participation and redress; security; transparency; use limitation. The VBMS-Fiduciary application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how veterans' information is used, stored, and protected.

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.

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, Mailing Address, Military Branch

Beneficiary Profile:
Veteran File Number, Veteran Name, Beneficiary Name, Social Security Number, Birth Date, Date of Death, Date of Incompetency, Email Address, Secondary Email Address, Home Phone Number, Cell Phone Number, Telephone Number 1-4, Accounting Number, Routing Number, Mailing Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country), Physical Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country), Fiduciary Name

Fiduciary Search:
Name, SSN, Date of Birth, Physical Address

Fiduciary Profile:
First Name, Middle Name, Last Name, SSN, Date of Birth, Email Address, Secondary Email Address, Primary Phone, Alternative Phone, Alternative Phone 2, File Number, SSN, Mailing Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country), Physical Address (Address Type, Street 1, Street 2, Street 3, City, State, Zip Code, Country)

Field Exam Report:
Beneficiary Name, Beneficiary's Social Security Number, Name of Veteran, VA File Number, Veteran's Social Security Number, Fiduciary Name, Name of preferred Fiduciary, Dependent Name

Accounting Audit Tool:
Beneficiary Name, Fiduciary Name

Misuse Record:
Beneficiary Name, Fiduciary 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.

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

In general, all the data will be retained for three years. All VA and VAMC provided information is destroyed at the end of the contract.
Recovery Audit System Files: Inputs- destroy/delete source data after data is entered into the master file or database and verified, or when no longer needed to support construction of, or serve as backup to, the master file or database, whichever is later.
Prior to decommissioning of system(s), AWS must receive written approval from the VA before any VA provided information is destroyed. Any data destruction done on behalf of the VA must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in GRS 4.2, https://www.archives.gov/files/records-mgmt/grs/grs-trs31.pdf.

As determined by the VA Records Management Officer, the PII data specifically stored by the VBMS-Fiduciary application does not meet the definition of "record" as defined by https://www.law.cornell.edu/uscode/text/44/3301 and therefore does not have an assigned disposition schedule.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

In general, these records are retained and disposed of in accordance with the General Records Schedule 3.1 and 3.2 (GRS 20), approved by National Archives and Records Administration (NARA) https://www.archives.gov/records-mgmt/grs.html and Veterans Benefits Administration Records Control Schedule VB-1, Parts I and II at https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc, https://www.benefits.va.gov/WARMS/docs/regs/RCS_II.doc.

As determined by the VA Records Management Officer, the PII data specifically stored by the VBMS-Fiduciary application does not meet the definition of "record" as defined by https://www.law.cornell.edu/uscode/text/44/3301 and therefore does not have an assigned disposition schedule.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 Electronic Media Sanitization, https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf, described in part below:
"(5) Media Sanitization (a) VA will comply with NIST 800-88 for the purposes of media sanitization on all IT equipment. (b) VA will use approved techniques or methods to dispose of, destroy, or erase VA information, consistent with VA retention guidelines and National Archives and Records Administration (NARA) approved records control schedules. This applies to originals as well as copies and archived records, including system logs that may contain PII/PHI."

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

VBMS-Fiduciary does not use any PII or PHI in the test, prod-test, or pre-production environments or for training or research, thus minimizing the risk of exposing PII. The IA team has automated scripts that run in these environments to test for the leakage of actual PII into an environment not authorized as such.

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.

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that the information maintained by VBMS-Fiduciary could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, VBMS-Fiduciary adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in GRS 3.1 (010, 011, 020), 4.3 (020), and 3.2 (030). However, as determined by the VA Records Management Officer, the PII data specifically stored by the VBMS-Fiduciary application does not meet the definition of "record" as defined by https://www.law.cornell.edu/uscode/text/44/3301 and therefore does not have an assigned disposition schedule.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Benefit Gateway Services (BGS)	BGS is the gateway into the Corp DB which was previously the authoritative source for most of the Veteran and Claim data for VBA.	Detailed data elements are too many to list and would be virtually everything to do with a Veteran, Veteran Demographics, Veteran Claims, Claim Adjudication, and Claim Award including Veteran File Number, Name, Social Security Number.	SOAP over HTTPS using SSL encryption and Certificate exchange

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
VBMS EFolder (Veterans Benefit Management System)	VBMS eFolder contains Veterans' eFolder to which VBMS-Fiduciary related correspondence is uploaded.	Veteran Benefit information documentation	REST Web Service API (HTTP)
VBMS ClaimsAPI	VBMS ClaimsAPI contains claims information necessary for processing within the VBMS-Fiduciary application.	Veteran Claims information	REST Web Service API (HTTP)
IAM (Identity Access Management)	IAM is management of the credentials used to match a logged-in user with the appropriate permissions for their role in VBMS-Fiduciary application.	PII – Identity Access Information for User access control: Name, Address, SSN (Data Encrypted)	REST Web Service API (HTTP)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data within the Department of Veterans' Affairs could happen and the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, need-to-know, transparency and use limitation.

Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know. Only personnel with a clear business purpose for accessing the information are allowed to access VBMS-Fiduciary and the information contained within.
The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication.

Section 5. External Sharing/Receiving and Disclosure

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

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Note: This question is #7 in the Privacy Threshold Analysis.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified***	***List the specific data element types such as PII/PHI that are shared/received with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external***	***List the method of transmission and the measures in place to secure data***

	program office or IT system		***sharing (can be more than one)***	
VBMS-Fiduciary does not share information with any programs outside the VA	N/A	N/A	N/A	N/A

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

VBMS-Fiduciary was designed, developed, deployed, and is operated and maintained within the requirements of OMB Memoranda M-06-15 Safeguarding Personally Identifiable Information and M-06-16 Protection of Sensitive Agency Information. Specifically, the VA has designated the Deputy CIO as the Senior Agency Official for Privacy (SAOP), and VBMS encrypts all data in transit, uses two factor authentications, time out functions, and event logging in accordance with VA6500 Rev 4.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:
Privacy Risk: N/A VBMS does not share information with systems outside of the VA

Mitigation: N/A

Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is 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.

The Department of Veterans Affairs does provide public notice that the VBMS system does exist from which the VBMS-Fiduciary application is accessible. VBMS-Fiduciary application is not publicly accessible, only via the VBMS system. 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 they individual read and understood the NOPP is scanned into each applicant's electronic file. When updates are made to the NOPP copies are mailed to all Veteran's beneficiaries. Additionally, new NOPPs are mailed to beneficiaries on a yearly basis and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records.
Additional notice is provided through this Privacy Impact Assessment, which is available online, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA System of Record Notices (SORNs) which are published in the Federal Register and available online: The System of record Notice (SORN) "Compensation, Pension, Education, and Rehabilitation Records-VA" 2019 58VA21/22/28 SORN located at https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf .

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

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

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

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?
This question is related to privacy control IP-1, Consent

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

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:
Privacy Risk: There is a risk that members of the public may not know that the VBMS-Fiduciary system exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Impact Assessment and the System of Record Notice.

Section 7. Access, Redress, and Correction

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

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

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction

unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

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).

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 question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Members of the public are not allowed access to VBMS-Fiduciary. An individual who wishes to determine whether a record is being maintained under his or her name in VBMS-Fiduciary 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.

Veterans and authorized parties have a statutory right to request a copy of or an amendment to a record in VA's possession at any time under the Freedom of Information Act (FOIA) and the Privacy Act (PA). VA has a decentralized system for fulfilling FOIA and PA requests. The type of information or records an individual is seeking will determine the location to which a request should be submitted. For records contained within a VA claims folder (Compensation and Pension claims), or military service medical records in VA's possession, the request will be fulfilled by the VA Records Management Center. Authorized requestors should mail or fax their Privacy Act or FOIA requests to: Department of Veterans Affairs, Claims Intake Center, P.O. Box 4444, Janesville, WI 53547–4444, Fax: 844– 531–7818, DID: 608–373–6690."

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 not notified if there is missing or inaccurate information in their record. An individual who wishes to determine whether a record is being maintained under his or her name in VBMS-Fiduciary 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. Requests should contain the full name, address and telephone number of the individual making the inquiry. (Per 58VA21/22/28 SORN)

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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Veterans and other beneficiaries may contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information. VBMS-Fiduciary receives information from other systems therefore veterans instead would have to go through the source system's protocols to correcting the data.

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.

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

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

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

Follow the format below:

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

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

Section 8. Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Access to VBMS-Fiduciary is controlled through form authentication and the following assigned user roles, each with unique combinations of view/edit privileges within the system.

- Fiduciary Program Support Analyst
- Fiduciary Legal Administrative Specialist
- Legal Instrument Examiner
- Lead Legal Instrument Examiner
- Fiduciary Service Representative
- Field Examiner
- Fiduciary Management Analyst
- Fiduciary Quality Review Team Specialist
- Fiduciary Coach/Assistant Coach
- Fiduciary Hub Manager/Assistant Manager

All users of the VBMS-Fiduciary are required to complete annual information system security training activities including security awareness training and specific information system security training. Annual training on VA Privacy and Information Security Awareness is tracked on the VA TMS.

Access to VBMS-Fiduciary working and storage areas is restricted to VA employees and authorized Contractors who must complete both the HIPAA and Information Security training using TMS. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), local Chief Information Officer (CIO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

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, ISO and OI&T approval must be obtained prior to access 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 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.

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. By policy, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

Access to computer rooms at the AWS facility is limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. VA furnished laptops and similar devices are protected with two-factor authentication and OS level encryption at rest.

Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at AWS facility is supervised and rigorously controlled.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, the VBMS program contractors who provide support to the system are required to complete a Moderate Background Investigation (MBI), complete annual VA Privacy and Information Security

and Roles of Behavior training via the VA's Talent Management System TMS. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.
VA contract employee system/application access is verified through VA Contract Officers Representative (COR) before access is granted to any contractor.

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

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

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

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

Yes, as a minor application on BIP, VBMS-Fiduciary inherits the BIP Authority to Operate (ATO) issued Jan 21, 2021. This ATO will expire on Jan 21, 2022. The FIPS classification is "HIGH".

Section 9. 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

ID	Privacy Controls
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.

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.06.16 11:12:11 -04'00'

Privacy Officer, Rita Grewal

Joseph Facciolli 148552

Digitally signed by Joseph Facciolli 148552
Date: 2021.06.11 11:18:50 -04'00'

Information System Security Officer, Joseph Facciolli

Gary W. Dameron 101941

Digitally signed by Gary W. Dameron 101941
Date: 2021.06.11 11:09:54 -04'00'

Information System Owner, Gary Dameron

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).

Notice of Privacy Practices

This 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 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.

PRIVACY ACT INFORMATION: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA Programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain or retain benefits. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us, your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefit for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine maximum benefits under the law. The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies.