Privacy Impact Assessment for the VA IT System called:

Veterans Benefits Management System (VBMS) Cloud Assessing

Veterans Benefits Administration (VBA)

Benefits, Appeals, and Memorials (BAM)

eMASS ID # 1021

Date PIA submitted for review:

9/12/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.Harvey@va.gov	202-461-8401
Information System Security Officer (ISSO)	Joseph Guillory	Joseph.guillory@va.gov	619-204-6840
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?".

Veterans Benefits Management System (VBMS) Cloud Assessing is an integrated web application intended to streamline Veteran's disability claims process by providing claims processors with an electronic, paperless environment in which to maintain, review, and make rating decisions for veterans' claims. VBMS is a system of systems that interconnects with many local and disparate software components. VBMS can be decomposed into systems of interconnectivity, layers within each information system, and software components that comprise and integrate these layers. The application is hosted in a cloud-based environment utilizing virtual servers to deliver Veteran's information and evidence for processing via a web browser. End-to-end claims processing provides functionality required for establishment, development, rating, award, and appeal of a claim. It is the intent of this effort to deliver VBMS incrementally using an agile development methodology based upon the priorities determined by the Office of Information Technology (OIT) and the Benefits, Appeals, and Memorials (BAM) program office.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

Veterans Benefits Management System (VBMS) Cloud Assessing is under the authority of the Benefits, Appeals, and Memorials (BAM) program office.

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

The VBMS system is used to administer compensation benefits and deliver disability compensation, a tax-free monetary benefit paid to Veterans with disabilities that are the result of a disease or injury incurred or aggravated during active military service.

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

Veterans Benefits Management System (VBMS) Cloud Assessing is a VA Controlled / non-VA Owned and Operated system owned and controlled by Benefits, Appeals, and Memorials (BAM).

2. Information Collection and Sharing

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

All Veterans and dependents of Veterans who filed claims will have information stored or processed by this system. The approximate number of Veterans and dependents is around 12,700,000.

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

VBMS is an electronic work environment (EWE) designed for processing compensation and pension claims and the purpose for collecting Veterans information is to process those claims correctly.

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

VBMS shares information with the Veterans Benefits Administration (VBA) through Compensation and Pension Record Interchange (CAPRI) Electronic software package. VBMS shares information with Data Access Services (DAS) that brokers data for the following systems: Compensation & Pension Record Interchange (CAPRI), Clinical User Interface (CUI), and Exam Management, Health Artifact & Image Management Solution (HAIMS). VBMS shares information with Performance Analysis & integrity (PA&I) to send Veteran and claim data and fetch exam data. VBMS shares information with VONAPP Direct connect (VDC) and the stakeholder enterprise ports (SEP) that are sister programs that both connect through DAS for Veteran data. VBMS shares information with Virtual VA (VVA) which is now replaced by FTI (Federal Tax Information) Capture includes a web application and an API to allow users to scan, index, and deliver FTI documents to the FFR (Federal Tax Information File Repository). VBMS shares information with VA Information Security Oversight Office (ISOO) / Clinical User Interface - CUI, Enterprise Veterans Self-service (EVSS) and Ebenefits connects unidirectionally through DAS to provide several services to the Veterans Relationship Management (VRM) program. These programs are also collectively referred to as the EVSS applications. VBMS shares information with Digits to Digits (D2D) because the D2D initiative is a data delivery service that allows accredited partners such as VSOs to use their current claim management systems to prepare claims and submit them to VBMS. VBMS shares information with Veterans Claims Intake Programs (VCIP) which VBMS provides an interface for third-party scanning vendors, collectively referred to as the VCIP, to upload scanned images of documents sent as part of the claims processing workflow. VBMS requires that document upload functionality includes the ability to extract document metadata. VBMS shares information with Benefit Gateway Services (BGS) which provides the bulk of the claims processing functionality that is not directly related to scanned document storage and routing, as well as a common security framework for authentication and authorization. VBMS shares information with Solution Made Simple (SMS) to gather documents that are uploaded through DAS.

G. Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

VBMS resides on the VAEC (Veterans Administration Enterprise Cloud) and therefore has no issues with synchronization. This is because of the multiple availability zones utilized by VAEC that provide this synchronization, redundancy, and replication.

3. Legal Authority and SORN

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

- 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
- 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. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

No, amendments or revisions to the SORN are not required.
Yes, the SORN does cover cloud usage.

4. System Changes

J. Will the completion of this PIA result in circumstances that require changes to business processes?

Completion of this PIA will not result in changes to existing business processes.

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

Completion of the PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

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

Other PII/PHI data elements:
Family Relation
Alias
File Number
Guardian Information
Benefit Information
System Log Files
Claims/Appeals

PII Mapping of Components (Servers/Database)

Veterans Benefits Management System (VBMS) Cloud Assessing consists of **four** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Veterans Benefits Management System (VBMS) Cloud Assessing** and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Database names are not identified in the VBMS application	Yes	Yes	• Name • Social Security Number • Date of Birth	Veteran data required to process	VA Network only which requires VPN access and 2

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

interconnection. Receiving systems manage internal information delivery as part of their receiving application			• Mother's Maiden Name • Personal Mailing Address • Personal Email Address • Personal Phone Number(s) • Financial Account Information • Medications • Race / Ethnicity • Tax Identification Number • Gender • Military History / Service Connection • Alias • Driver's License Number • Family Relation • Guardian Information • Benefit Information • Medical Records • Claims/Appeals • File Number	claims and pay benefits	Factor Authentication thru the Trusted Internet Connection (TIC) Gateway

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The VBMS system receives information directly from the application's user interface (UI) and electronically via web services. VBMS receives information from Benefit Gateway Services (BGS), Common Security Services (CSS), FTI (Federal Tax Information) Capture, Master Veteran's Index (MVI), Clinical User Interface (CUI), Digits to Digits (D2D), Enterprise Veteran Self Service (EVSS), VONAPP Direct connect (VDC), Stakeholder Enterprise Portal (SEP), eBenefits, and Customer Relationship Management (CRM), Solutions Made Simple (SMS), Performance Analysis & Integrity (PA&I), Compensation & Pension Record Interchange (CAPRI), Exam Management, Health Artifact & Image Management Solution (HAIMS), Veterans Claims Intake Programs (VCIP), and VBMS Fiduciary.

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.

Scanning vendors are under the Veteran's Claims Intake Programs (VCIP) which currently has uses the contractors SMS. VCIP is used to scan-in paper documents that exist for veterans that were used during the legacy paper claim filing process. The VBMS user interface assists with veteran claim data (filed by Veteran Service Organization (VSO), veterans, or other sources), veteran exam results, and additional evidence in relation to filed claims.

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

VBMS does create information for claims from VBMS Fiduciary, Performance Analysis & integrity (PA&I), and others listed in the answer of 1.2a.

1.3 How is the information collected?

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

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

Information is collected from VBA claims processers in the Region Offices (RO) as input through the web UI. Scanning vendors, SMS and CSRA, scan in paper documents that exist for veterans remotely via web services into the VBMS document repository. VBMS receives claims information electronically via web services from VA hospitals and health care providers.

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?

Information is not collected on a form.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that

receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

As information is imported from VA healthcare providers, the accuracy is verified by the original source. Veteran information that is retrieved from VBA Corporate Database (CorpDB or CRP) is validated via BGS and veteran information queried through the UI is validated via Master Veteran Index (MVI) Prior to any award or entitlement authorization(s) by the VBMS, the veteran record is manually reviewed, and data validated by the Veteran Service Representative (VSR) and the Rating Veteran Service Representative (RVSR) to ensure correct entitlement has been approved.

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 does not check for accuracy by accessing a commercial aggregator of information.

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

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

- 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
- 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

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: VBMS collects Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). This information is specifically collected for the purpose of VBMS as a system. It is an absolute requirement for the efficacy of VBMS. 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 is built on the existing VBA Common Security System (CSS) that controls user authentication and role-based permissions. Permissions are only given after a request and approval of that request by an Information System Owner (ISO). Because of the nature of VBMS, information is collected from health care providers, VBA claims, and scanning vendors. 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 provides additional security to VBA CSS for both integrity and confidentiality which will prevent unauthorized users from gaining access to any data. Additionally, VBMS is an internally hosted application meaning that only the authorized user can access VBMS and those users have to be on the VA network which insulates VBMS from any outside/public access. VBMS employs 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 that will be used in support of the program's business purpose.

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

PII/PHI Data Element	Internal Use	External Use
Name	Used to identify Veteran	Used to identify Veteran
Social Security Number	Used to verify the identity of the Veteran	Used to verify the identity of the Veteran
File Number	Used as an identification number for a Claim/Appeal for a Veteran	Used as an identification number for a Claim/Appeal for a Veteran
Date of Birth	Used to identify the Veteran	Not used
Mother's Maiden Name	Used to verify the identity of the Veteran	Not used
Personal Mailing Address	Used to correspond with the Veteran	Not used
Personal Email Address	Used to correspond with the Veteran	Not used
Personal Phone Number(s)	Used to correspond with the Veteran	Not used
Financial Information	Used as a reference for the Veteran's account	Not used
Medications	Used to track medical information	Not used
Race/Ethnicity	Used to verify the identity of the Veteran	Not used
Tax Identification Number	Used as a file number for Veteran	Not used
Gender	Used to verify the identity of the Veteran	Not used
Military History/Service Connection	Used to determine benefits eligibility	Not used
Alias	Used to verify the identity of the Veteran	Not used
Certificate/License Numbers	Used to verify the identity of the Veteran	Not used
Family Relation	Used for Veteran's family benefits	Not used

Guardian Information	Used to verify if Veteran's family member has guardian	Not used
Benefit Information	Used to determine benefit eligibility	Not used
Medical Records	Used to track medical information	Not used
System Log Files	Information collected by the system	Not used
Claims/Appeals	(Claim) Used as a formal application for a Veteran seeking benefits related to a service-connected disability or other eligible condition/ (Appeal) Used as part of the process a Veteran may take if they disagree with a benefit or claim	Not used

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

The analysis that VBMS conducts is presented as a Scorecard which is created from active claim statistics.

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.

VBMS uses Scorecard to provide VBA with active claims statistics for a given regional office. This produces data that will be used to determine rulesets for National Work Queue (NWQ) to route claims to other regional offices. VBMS uses advanced analytics to suggest body systems to users of VBMS-R (Ratings) based on large historic claim data sets. This produces the suggested body system code for raters to use for the appeals and awards process.

2.3 How is the information in the system secured?

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

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

All sensitive and confidential data is encrypted using FIPS 140-2 compliant AES-256 encryption algorithms in transit and at rest. The information includes objects in VAEC AWS GovCloud s3 buckets, Elastic Block Store (EBS) volumes, and databases. AWS uses EBS encryption (AES-256 algorithms) which uses AWS Key Management Service keys when creating encrypted volumes and snapshots.

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

No, all sensitive and confidential data is encrypted using FIPS 140-2 compliant AES-256 encryption algorithms in transit and at rest. The information includes objects in VAEC AWS GovCloud s3 buckets, Elastic Block Store (EBS) volumes, and databases. AWS uses EBS encryption (AES-256 algorithms) which uses AWS Key Management Service keys when creating encrypted volumes and snapshots.

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

VBMS inherits some of the implementation of this control from VA OIT and AWS GovCloud High accreditation package. Documents are transmitted to VBMS through electronic system interfaces and the VBMS Web UI document upload feature. All interfaces for uploading documents are protected by A&A (Authentication and Authorization) controls at the network and application layers. VBMS components guarantee the confidentiality and integrity of data transmissions between VBMS and other parties with IP security between the communicating nodes at the transport layer. VBMS uses NFS for file sharing within database clusters.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

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

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

Yes

2.4c Does access require manager approval?

Yes

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

Yes

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

The VBMS application team has implemented the required security controls based on the tailoring guidance of NIST (National Institute of Standards and Technology) 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.

The ISO, ISSO, and PO (Privacy Officer) ultimately share responsibility assuring the safeguards for PII.

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*

Name, Social Security Number, Date of Birth, Mother's Maiden Name, Personal Mailing Address, Personal Email Address, Personal Phone Number(s), Financial Account Information, Current Medications, Race/Ethnicity, Tax Identification Number, Gender, Military History/Service Connection, Alias, Driver's License Number, Family Relation, Guardian Information, Benefit Information, Medical Records.

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. **The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.** If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

VBMS adheres to the NARA General Records Schedule per VA data retention policies.

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

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

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

Yes

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

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

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

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

VBMS adheres to the NARA General Records Schedule.

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 does not use any PII/PHI in design/development process or Dev/Stage environments. Access to PII/PHI is only available in the production environment of VBMS.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that the information maintained by VBMS 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 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 General Records Schedule 20.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Benefit Gateway Service (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	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Email Address • Financial Information • Medications • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	Simple object access protocol (SOAP) over HTTPS using SSL encryption and Certificate Exchange
Data Access Services (DAS)	DAS is the common service that exchanges information with other agencies both within VA and external to VA	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Email Address • Financial Information • Medications • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	SOAP over HTTPS using SSL encryption and Certificate Exchange
Veterans Benefits Administration Performance Analysis & integrity (PA&I)	PA&I uses a daily extract of claim and work item data to produce reports and metrics for VBMS	• System Log files • Name • Social Security Number • Date of birth • Mother's Maiden Name • Personal Mailing Address • Personal Email Address • Financial Information • Medications • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	Secure File Transport Protocol (SFTP)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Veterans Benefits Administration VONAPP Direct Connect (VDC) and the Stakeholder Enterprise Portal (SEP)	Veterans Online Application (VONAPP) Direct Connect (VDP) and the Stakeholder Enterprise Portal (SEP) allow claimants to file disability compensation and dependency applications directly to SOO (Statement of Objective) via eBenefits. VBMS is the document repository for claims materials submitted through VDC.	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Email Address • Financial Information • Medications • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	VDP and SEP are sister program that both connect through DAS using simple object access protocol over SSL. This is encrypted traffic secured by certificate exchange
Federal Tax Information (FTI) Capture	FTI (Federal Tax Information) Capture includes a web application and an API to allow users to scan, index, and deliver FTI documents to the FFR (Federal Tax Information File Repository)	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Email Address • Financial Information • Medications • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	FTI Capture connects through DAS using SOAP over SSL. This is encrypted traffic secured by Certificate Exchange.
VA Information Security Oversight Office (ISOO) / Clinical User Interface - CUI	CUI provides exam responses unidirectionally to VBMS Core to populate Ratings, Correspondence, and Awards data	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Email Address • Financial Information • Medications • Race/Ethnicity • Tax Identification Number • Gender	CUI connects unidirectionally through DAS using SOAP over SSL. This is encrypted traffic secured by 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 PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		• Military History/Service Connection	
Veterans Benefits Administration Enterprise Veteran Self-Service (EVSS) and Ebenefits	EVSS and eBenefits both allow Veterans to initiate and submit a claim establishment on their own behalf through VMBS to BGS.	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Email Address • Financial Information • Medications • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	EVSS / eBenefit connects through DAS using SOAP over SSL. This is encrypted traffic secured by Certificate Exchange.
Veterans Benefits Administration Digits to Digits (D2D)	D2D is a data delivery service built to enable the VSOs to electronically submit data and related attachments from its CMS to VA systems using a standardized and centralized method.	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Email Address • Financial Information • Medications • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	D2D connects through DAS using SOAP over SSL. This is encrypted traffic secured by Certificate Exchange.
Scanning Vendor: Solutions Made Simple (SMS)	Scanning vendors turn literal tons of paper files into scanned images of paper documents and attach them as evidence to Veteran's ID and claim numbers.	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Email Address • Financial Information • Medications • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	Documents are uploaded through DAS using SOAP over SSL. This is encrypted traffic secured by Certificate Exchange, and are only referenced by metadata.

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Veterans Benefits Administration (VBA)	Information is shared across VBA to facilitate Veterans benefits claim processing.	• Name • Social Security Number • Date of Birth • Mother's Maiden Name • Personal Mailing Address • Personal Email Address • Financial Information • Medications • Race/Ethnicity • Tax Identification Number • Gender • Military History/Service Connection	Compensation and Pension Record Interchange (CAPRI) electronic software package.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with 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 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: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with External Organizations

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

	specified program office or IT system		***permit external sharing (can be more than one)***	
GovCIO, LLC – Paper Mail Conversion Management Service	For both paper and electronic modalities, GovCIO will handle source material intake, handling, and preparation; data extraction; document indexing, conversion, and imaging. Upon completion of mail processing, images, with associated data, will be integrated and uploaded to VA systems.	• Name • Social Security Number • File Number	MOU / ISA	HTTPS over VPN

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: PII, including personal contact, service, and benefits information could be released to unauthorized individuals. Additionally, misspelling a Veteran's name could result in the wrong data being displayed to the user.

Mitigation: Outside agencies provide their own level of security controls such as access control, authentication, and user logs in order to prevent unauthorized access. The ISA/MOUs between VBMS and external agencies establish the security requirements for the VA and the external agency. The VA and external systems are protected by the Moderate system certification level which ensures criticality defined by FIPS 199. The authorization process is completed for IBS and external agencies and an Authority to Operate (ATO) has been approved. The security controls identified by NIST SP 800-53 for a moderate system are implemented to protect IBS and external agencies.
All personnel with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior (ROB) annually. IBS users and applications adhere to all information security requirements established by VA OIT and information is shared in accordance with VA Handbook 6500. All personnel accessing Veteran's information must first have a successfully adjudicated fingerprint check conducted by the Federal Bureau of Investigation (FBI). Individual users are given access to Veterans' data through the issuance of a user ID and password and using a Personal Identity Verification (PIV) card for two-factor authentication.

Section 6. Notice

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

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

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

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

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.

This Privacy Impact Assessment (PIA) also serves as notice of the 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."

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

The System of Record Notices (SORN) 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

Please provide response here

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

VA gathers or creates these records in order 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 Notices (SORN) 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

This Privacy Impact Assessment (PIA) also serves as notice of the 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."

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 health care benefits. Veterans and their family or guardian (spouse, children, parents, grandparents, etc.) may not decline or request their information not be included as part to determine eligibility and entitlement for VA compensation and pension benefits. Veterans and/or their family may 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 in order 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 System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: Individuals may not be provided an opportunity to provide consent for any secondary use of information such as use of collected information for marketing..

Mitigation: The VA mitigates this risk by providing the Notice of Privacy Practice (NOPP) document.

Section 7. Access, Redress, and Correction

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

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

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

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

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.

Contact local VA Release of Information Office.

FOIA Request
To file you must "Register" with PAL.
Submit a proper request.
Access the VA FOIA Reading Room for previously released documents.
Request status updates on your submitted request.
Learn about processing fees, fee waivers, and requester categories.

Privacy Act Request
There are **two options** to submit a Privacy Act request, either:

- Privacy Act requests can be made by completing the **entire** VA Form 20-10206, Freedom of Information Act or Privacy Act
- Send a written request to the Centralized Support Division, including the individual's Social Security number or C-File number may aid in the identification of records.

Centralized Support Division mailing address and email:
Department of Veterans Affairs
Evidence Intake Center
P.O. Box 4444
Janesville, WI 53547-4444
FOIA.vbarmc@va.gov.
Note: When sending a request by email, the signed request **must** be included as an email attachment and include the wet signature.

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 procedure is covered under the System of Record Notices (SORN) as well as provide information listed in question 7.1a.
58VA21/22/28: *Compensation, Pension, Education, and Rehabilitation Records- VA,*
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

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

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

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

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

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

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 Rehabilitation 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.

Veterans and other beneficiaries may contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals records may be incorrect in the system that may delay the process of filing a claim.

Mitigation: VBMS does not provide individual access to records. By publishing this PIA, and the applicable SORN, the VA informs individuals on how to access, redress, and make record correction.

Section 8. Technical Access and Security

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

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

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

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.

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

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

Yes, 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. 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?

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 05/04/2023
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 07/24/2023
5. *The Authorization Termination Date:* 07/23/2025
6. *The Risk Review Completion Date:* 07/24/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Section 9 – Technology Usage

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

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

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

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)*

VBMS utilizes the VA Enterprise Cloud (VAEC) as it's cloud service provider.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

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.

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.

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).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

MARVIS HARVEY

Digitally signed by MARVIS HARVEY
Date: 2024.12.11 06:14:57 -06'00'

Privacy Officer, Marvis Harvey

JOSEPH GUILLORY

Digitally signed by JOSEPH GUILLORY
Date: 2024.12.10 13:09:01 -08'00'

Information System Security Officer, Joseph Guillory

CHRISTINA LAWYER

Digitally signed by CHRISTINA LAWYER
Date: 2024.12.11 07:27:13 -05'00'

Information System Owner, Christina Lawyer

APPENDIX A-6.1

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

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

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

https://department.va.gov/privacy/privacy-impact-assessments/

HELPFUL LINKS:

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

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

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

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

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