Privacy Impact Assessment for the VA IT System called:

VBMS Exam Management

Veterans Benefits Administration (VBA)

Benefits, Appeals, and Memorials (BAM)

eMASS ID# 2053

Date PIA submitted for review:

12/11/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.Harvey@va.gov	202-461-8401
Information System Security Officer	Joseph Facciolli	Joseph.Facciolli@va.gov	215-983-5299
Information System Owner	Christina Lawyer	Christina.Lawyer@va.gov	518-210-0581

Abstract

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

The Veterans Benefits Management Systems (VBMS) Exam Management (Exam Mgmt) application is an Application Programming Interface (API) that provides exam message details to VBMS User Interface (UI) users. It is a stand-alone service hosted in VA Enterprise Cloud (VAEC) Amazon Web Services (AWS). This API accesses data stored in the VBMS UI monolithic database and inherits the Authority to Operate (ATO) for the VBMS Core application.

Overview

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

1 General Description

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

VBMS Exam Mgmt is a minor application responsible for providing exam message details to VBMS UI.

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

The VBMS Exam Mgmt application is owned, built, and managed by the Benefits, Appeals, and Memorials (BAM) program office. This is a VA Owned and a VA Operated system.

2. Information Collection and Sharing

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

There are approximately 3.4 million veterans in the VBMS Exam Mgmt application that are involved with medical exams to support benefit claims. A typical client is a veteran seeking VA benefits. The purpose of VBMS Exam Mgmt is to allow VA Employees to collect medical information related to the veteran's contentions. This information is used to rate the severity of a specific veteran claim and used to determine the correct benefits for distribution.

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

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

The application accesses data stored in the VBMS Core database related to exam management transactions.

- Name - Used to identify the claimant or Veteran
- Social Security Number (SSN) - Used as File Number
- Date of Birth - Used to uniquely identify the claimant or Veteran
- Personal Mailing Address - Used to provide official correspondence to claimant or Veteran, and identify field examiner proximity
- Personal Phone Number(s) - Used to communicate with claimant or Veteran appointment scheduling
- Medical Records - Used by field examiners for claimant or Veteran medical information
- Gender - Used by field examiners for claimant or Veteran medical information
- Military History/Service Connection - Used by field examiners for claimant or Veteran medical information
- File Number - Used to uniquely identify claimant or Veteran
- Employee ID and Station - Collected and used to person requesting medical examination in the event additional information is needed

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

The IT system facilitates internal information sharing across multiple components to support VA benefits and related services. For example, the Veterans Benefits Administration (VBA) and Medical Disabilities Exam Office (MDEO) exchange sensitive

data elements, such as names, Social Security Numbers, medical records, and military service history. This data sharing occurs via secure communication protocols like HTTPS to ensure data integrity and confidentiality. The Benefits Integration Platform (BIP) serves as the backbone for these operations, hosting applications in the VA Enterprise Cloud (VAEC) on AWS. Leveraging technologies like Red Hat OpenShift, Kubernetes, and AWS Virtual Private Clouds, BIP ensures secure application development and segmented storage of data. It supports core VA systems like VBMS Fiduciary and Memorial Benefits Management, enhancing information sharing while maintaining strict security controls.

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

No

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

The systems infrastructure is only managed and administered from one site

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

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

Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. § 501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

I. What is the SORN?

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

J. SORN revisions/modification

The SORN was last revised on November 8, 2021.

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

No

4. System Changes

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

☐ Yes

☒ No
if yes

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

☐ Yes
☒ No
if yes

Section 1. Characterization of the Information

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

1.1 Information collected, used, disseminated, created, or maintained in the system.

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

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

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

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

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

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

Other PII/PHI data elements: File Numbers, Employee ID, Station

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

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

The information is provided by individuals during the application process for VA benefits and services, including personal details such as name, Social Security Number, and contact information. Additional data, such as medical records and military history, is shared internally between VA offices, such as the Veterans Benefits Administration (VBA) and Medical Disabilities Exam Office (MDEO), using secure transmission protocols like HTTPS. This data is managed on the Benefits Integration Platform (BIP), a secure cloud-based application platform, which enforces robust security controls and utilizes advanced tools to ensure efficient and secure processing across VA systems.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

All data collected by Exam Mgmt is used to provide accurate exam message details to the VBMS end users.

Veterans Benefits Management System (VBMS) is the primary user interface for VBA users. VBMS provides claim and document-related information.

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

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

The application does not create information.

1.3 Methods of information collection

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

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

The VBMS Exam Mgmt application collects information via HTTPS protocol.

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 Information checks for accuracy, and how often will it be checked.

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

In the Secure Enclave, Pension Centers follow standard operating procedures (SOPs) to conduct quality control on each claim's data. Claim-level checks are completed before awarding benefits and random samples are collected monthly for additional review by quality control specialists.

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?

No

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

The System of Record Notice (SORN), *VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records–VA* (58VA21/22/28) (Nov. 8, 2021) is available at https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf. Under the Freedom of Information Act (5 U.S.C. § 552a, as amended by Public Law No. 104-231) and Privacy Act of 1974, the IRS memo FD698-FED-AWS GovCloudL-031020 establishes legal authority for the VA and IRS to share Federal Tax Information (FTI), as specified in IRC §6103(l)(7) and §6103(b)(6). The information-sharing agreement between the IRS and VA is documented in DART 52.

For the Veteran eFolder in Virtual VA (VVA), which will contain FTI documents, the Secretary of Veterans Affairs has set guidelines under 38 U.S.C. § 8111 ("Sharing of VA and DoD Health Care Resources") and 10 U.S.C. § 1104 ("Resource Sharing with the VA"), incorporating the Economy Act (31 U.S.C. § 1535) to support statute implementation.

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The system collects, processes, and retains PII and PHI on Veterans and VA Employees. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: Data is stored securely within an AWS enclave with access safeguarded by industry-standard authentication and authorization protocols. Secure Sockets Layer/Transport Layer Security (SSL/TLS) encryption is applied to protect data both in transit and at rest.

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 the claimant or Veteran	N/A
Social Security Number	Used as File Number	N/A
Date of Birth	Used to uniquely identify the claimant or Veteran	N/A
Personal Mailing Address	Used to provide official correspondence to claimant or Veteran, and identify field examiner proximity	N/A
Personal Phone Number(s)	Used to communicate with claimant or Veteran appointment scheduling	N/A
Medical Records	Used by field examiners for claimant or Veteran medical information	N/A
Gender	Used by field examiners for claimant or Veteran medical information	N/A
Military History/Service Connection	Used by field examiners for claimant or Veteran medical information	N/A
File Number	Used to uniquely identify claimant or Veteran	N/A
Employee ID	Collected and used to contact person requesting medical examination in the event additional information is needed	N/A
Station	Collected and used to contact person requesting medical examination in the event additional information is needed	N/A

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

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

VBMS Exam Management does not perform any kind of data analysis or run analytic tasks. Data will only be stored in the secure enclave; no new data will be created or analyzed.

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

The system does not create or generate new information about an individual. It only processes and manages existing data that has already been collected through official channels. No new records are created, and no additional actions—positive or negative—are taken based on newly derived data. Government employees who make determinations about individuals will only have access to the original data that has already been collected and documented, ensuring no unintended consequences arise from system processing.

2.3 How the information in the system is secured.
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Secure Socket Layer/Transport Layer Security (SSL/TLS) measures are in place to protect data in transit and at rest.

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

Data is hosted in AWS and is encrypted both in transit and at rest via SSL/TLS.

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

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

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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?

Access to Personally Identifiable Information (PII) and Protected Health Information (PHI) within the VBMS Exam Management system is determined based on job responsibilities and the "need-to-know" principle. Users must be registered within VA systems and granted authorization based on assigned user roles. Before access is granted, users must complete required security and privacy training, and obtain approval through the VA's Electronic Permission Access System (ePAS).

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

Yes, criteria, procedures, controls, and responsibilities regarding access to this system are documented in various sites which are but not limited to TMS, GRC tool, and SharePoint sites.

2.4c Does access require manager approval?

Yes

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

Yes, data modifications are audited. The application is used to display PII and is transmitted via SSL encrypted networks. Access to the data is restricted to logged in users with the proper authorization to view.

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

The Information System Security Officer (ISSO) is ultimately responsible for ensuring that all PII and PHI safeguards are properly implemented and maintained within the system. The ISSO ensures compliance with security protocols, monitors system safeguards, and responds to potential risks.

Additionally, all VA employees and contractors with access to Veteran data are required to complete annual VA Privacy and Information Security Awareness Training and Rules of Behavior training. Users with access to Federal Tax Information (FTI) must also complete Internal Revenue Service (IRS) Publication 1075 training via the VA's Talent Management System (TMS 2.0), which tracks compliance.

Failure to follow security protocols may result in disciplinary action, including loss of access, suspension, or termination, depending on the severity of the violation.

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 secure enclave, all data is retained and stored in the repository. BIP follows VA Directive 6309 to ensure that the collection of information is needed; is not unnecessarily duplicative; reduces, to the extent feasible, the burden on respondents; is written in clear and understandable terms; is to be implemented in a way consistent with existing reporting and record keeping practices and that the records are retained for the length of time outlined within the record keeping requirement (General Records Schedule or Records Control Schedule). System record-keeping practices ensure that records are retained for the duration specified in the applicable record-keeping requirements such as the General Records Schedule or Records Control Schedule. VA follows its Record Control Schedule and the National Archives and Records Administration (NARA) General Records Schedule (GRS) for records retention and disposition.

3.2 How long is information retained?

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

The Exam Management claims files are electronically imaged and retained indefinitely as permanent records by the VA or transferred to the National Archives and Records Administration (NARA) for historical preservation. Paper copies are destroyed three years after the final adjudication of a claim or appeal, provided there are no pending related claims or appeals. This process follows the Records Control Schedule VB-1, Part 1 Section XIII, Item 13-052.100, as authorized by NARA. The VA employs comprehensive quality control measures, including random sampling, independent audits, and 100% review, to ensure the accuracy and completeness of electronic records before any paper copies are destroyed. SORN section: POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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

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

Yes

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

The retention schedule, series, and disposition authority for records are outlined under the "POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS" section of the SORN (https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf). Claims files are electronically imaged and stored indefinitely as permanent records by the VA or transferred to NARA for historical preservation. Paper copies, reclassified as duplicate non-record-keeping copies, are destroyed three years after the final adjudication of a claim or appeal, provided there are no related pending claims or appeals. This process adheres to Records Control Schedule VB-1, Part 1 Section XIII, Item 13-052.100, as authorized by NARA. The VA ensures the accuracy and completeness of electronically imaged records through rigorous quality control measures, including audits and 100% reviews. Additionally, temporary automated storage media are retained until a claim is decided, after which they are destroyed, in compliance with NARA-approved disposition authorizations.

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

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

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

then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

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

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

Real data is not used for research, testing, or training

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

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

Follow the format below:

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

Mitigation: Data retention follows established schedules ensuring PII/PHI is kept only as long as necessary to meet system purposes and legal requirements. Access is restricted to authorized personnel, and all employees with access complete privacy training to maintain data security and integrity.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **Exam Management** consists of **2** key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Exam Management and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
Veterans Benefits Administration	Yes	No	• Name • Date of Birth • File Number • Personal Mailing Address • Personal Phone Number(s) • Full Social Security Number • Medical Records • Gender / Sex	All data collected by VBMS Exam Management is used to provide accurate exam message details to VBMS end users.	Secure Socket Layer (SSL)/ Transport Layer Security (TLS)

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

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

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

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

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

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

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
VBMS Core	All data collected by VBMS Exam Management is used to be able to provide accurate exam message details to VBMS end users.	• Name • Full Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Medical Records • Gender / Sex • Military History/Service Connection • File Number • Employee ID • Station	Hyper-Text Transport Protocol – Secure (HTTPS)
Medical Disabilities Exam Office (MDEO)	All data collected by VBMS Exam Management is used to be able to provide accurate exam message	• Name • Full Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s)	Hyper-Text Transport Protocol – Secure (HTTPS)

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
	details to VBMS end users.	• Medical Records • Gender / Sex • Military History/Service Connection • File Number • Employee ID • Station	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

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

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA Employees to include employee security and privacy training along with required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***

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: Not applicable as there is no sharing of information outside of VBA or VA with external parties

Mitigation: Not applicable as there is no sharing of information outside of VBA or VA with external parties

Section 6. Notice

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

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

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

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

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

Additionally, individuals are notified through multiple channels:

1. The Notice of Privacy Practices (NOPP), provided during the application process for benefits, explains the collection and use of protected information. Veterans sign an acknowledgment confirming receipt and understanding of the NOPP which is scanned into their electronic records. Updates to the NOPP are mailed annually to beneficiaries.
2. A Privacy Act Statement accompanies the forms used for data collection ensuring individuals are informed of their rights and the purpose of the data collected.
3. This PIA itself serves as an additional notice, publicly available per the eGovernment Act of 2002, ensuring transparency. Veterans can access this PIA through the VA's official website or the Federal Register. These notices collectively inform individuals about the collection and use of their data and are referenced in Appendix A of this PIA.

6.1b If notice was not provided, explain why.

Notice is provided as outlined in the answer to question 6.1a above.

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

The notice provided at the time of collection is explicit and comprehensive, ensuring that individuals are fully informed about how their information is collected, used, and safeguarded. Veterans are notified through the NOPP, Privacy Act Statements, and the SORN, which detail the scope, purpose, and retention of their data. This ensures transparency and accountability in compliance with federal privacy requirements. This PIA also serves as a publicly accessible notice, further reinforcing that the collection and use of data align with the intended purpose of administering veteran benefits. These measures ensure that veterans are clearly and proactively informed, addressing any risks associated with the implicit nature of prior explanations.

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.

Yes, individuals have the opportunity and right to decline to provide information; however, declining to provide the requested information may result in the inability to process their claim for benefits. The collection of information is necessary to determine eligibility and administer the benefits for which the individual is applying. This requirement is communicated through the Privacy Act Statement included on the forms which explains the purpose of the data collection and the consequences of withholding information. While providing information is voluntary, the inability to provide necessary information may result in a denial of services or benefits as the VA cannot adjudicate claims without essential supporting data.

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.

Individuals provide consent for the use of their information through their acknowledgment of the Notice of Privacy Practices (NOPP) and the Privacy Act Statement included in the application process. These notices inform individuals about the purposes for which their data will be used and the systems where the data will be stored such as the VBMS Core system. Consent is given at the time of filing a claim or application for benefits, covering all authorized uses necessary to adjudicate and administer benefits. If an individual wishes to withdraw consent or inquire about

the specific use of their information, they may do so through established redress mechanisms including contacting the VA Privacy Office or submitting a written request to amend or limit data use as outlined in the Privacy Act and VA's data management policies.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

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

Privacy Risk: There is a risk that individuals may not receive adequate notice about the collection, use, or dissemination of their information, potentially leaving them unaware of its purpose or their rights regarding consent.

Mitigation: The VA addresses this risk by providing a Privacy Act Statement at data collection, the Notice of Privacy Practices (NOPP), the System of Record Notice (SORN) published in the Federal Register, and a publicly accessible Privacy Impact Assessment (PIA). These measures ensure transparency and inform individuals about the use of their information.

Section 7. Access, Redress, and Correction

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

7.1 The procedures that allow individuals to gain access to their information.

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

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

Procedures for individuals to access their information are outlined in the System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (November 8, 2021), available at this link https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf. Individuals may request access under the Freedom of Information Act (FOIA) or the Privacy Act by contacting their local VA Regional Office or submitting a Privacy Act Request via VA Form 20-10206. Written requests can also be mailed to the VA Centralized Support Division. For FOIA requests, individuals must register through the VA Public Access Link (PAL). For more information, individuals can refer to the VA FOIA Reading Room.

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

This system is not exempt from the access provisions of the Privacy Act. Individuals have the right to request access to their records as detailed in the SORN.

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

This system operates under the Privacy Act and the procedures outlined in 7.1a apply.

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.

Individuals can correct inaccurate or erroneous information by submitting a request to their local VA Regional Office or VHA center. The process follows guidelines outlined in the SORN and the VA's Privacy Act procedures. Requests may be submitted using VA Form 20-10206 or through direct written communication to the VA Centralized Support Division. Each request is reviewed by the appropriate Privacy Officer or System Manager.

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

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

Individuals are notified of correction procedures through multiple channels:

- At Collection: Privacy Act Statements on forms provide information about access and correction rights.

- SORN Notification: The SORN "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" explains the procedures for correcting records.

- VA Regional Offices: Veterans can contact their local VA office or VHA center for further guidance.

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.

Redress is provided under the Privacy Act and FOIA. Veterans and beneficiaries can access and correct their information through formal requests to the VA Regional Office or VHA centers. Additionally, individuals can contact the VA Centralized Support Division for support. For systems without direct access, corrections can be requested via mail, email, or in person through official VA channels, ensuring accuracy.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals whose information is used by this system may not be fully aware of the procedures for accessing, correcting, or contesting their records. This lack of awareness could lead to data inaccuracies that impact claims processing and benefits

determination.

Mitigation: The VA mitigates this risk by:

1. Publishing a Privacy Impact Assessment (PIA) and the applicable SORN, providing detailed procedures for accessing and correcting information.
2. Including Privacy Act Statements on all forms used for data collection ensuring individuals are informed at the point of collection.
3. Offering assistance through VA Regional Offices and the VA Centralized Support Division, with contact information provided in the PIA and SORN.
4. Ensuring comprehensive training for staff to guide individuals seeking access or corrections.

These measures enhance transparency and provide individuals with clear, actionable steps to address concerns about their records.

Section 8. Technical Access and Security

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

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

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

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

Access to the system follows VA Handbook 6500 protocols and is requested using the Electronic Permission Access System (ePAS). Individuals submit access requests based on their job duties and "need-to-know" principles. These requests require approval from the user's supervisor, Information Security Officer (ISO), and the Office of Information Technology (OIT) before access is granted. Access is secured using two-factor authentication, including a Personal Identity Verification (PIV) card and a complex password. Once inside the system, users are restricted to accessing only the information necessary for their role.

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. No external agency users are granted access. Criteria for sharing Personally Identifiable Information (PII) are established by the VA in accordance with applicable federal laws and regulations, as outlined in VA privacy policies.

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

The system includes the following roles:

- End-users: Individuals with access to perform routine tasks, such as tracking medical claims.
- Read-only users: Users who can view information but cannot modify or update records.
- Administrative users: Individuals with elevated privileges to manage system settings, perform maintenance, and support operations.
- Access levels are determined based on job responsibilities and are managed through the Common Security User Management (CSUM) application.

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

Yes, VA contractors have access to the system and PII. Access is granted on a "need-to-know" basis and contractors are subject to the same strict security and privacy protocols as VA employees.

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

Contractors support the production environment by performing tasks such as system development, testing, patching, upgrading, and administration. These roles are critical to ensuring the operational integrity of the system.

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

Yes, all contractors with access to the system are required to sign confidentiality agreements as part of their onboarding process. These agreements are maintained to ensure compliance with privacy and security policies.

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

Yes

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Yes, contractors are required to sign Non-Disclosure Agreements (NDAs) before accessing the system. NDAs are reviewed and maintained by the VA Contract Officers Representative (COR). Contractors must complete a Moderate Background Investigation (MBI) and annual VA Privacy and Information Security training. Contractors are granted access only for tasks directly related

to system maintenance and operations. Privacy roles and responsibilities are established to limit access based on user roles ensuring contractors only access the PII necessary for their duties.

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.

A contractor Production Operations team will support the BIP Exam Management production environment. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS). VBA end users of the system must take annual FTI awareness and protection training as outlined in IRS Publication 1075. This training must be completed via the VA's Talent Management System 2.0 (TMS) and compliance is tracked through the TMS 2.0 system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Not Yet Approved
2. *The System Security Plan Status Date:*
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 11/30/2023
5. *The Authorization Termination Date:* 11/30/2025
6. *The Risk Review Completion Date:* 11/30/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Section 9 – Technology Usage

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

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

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

(MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

VBMS Exam management utilizes the VA Enterprise Cloud (VAEC) AWS Government and is FedRAMP approved operating on a Software as a Service (SaaS) model.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). ***(Refer to question 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

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).

This system does not use Robotic Process Automation (RPA)

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

MARVIS HARVEY

Digitally signed by MARVIS HARVEY
Date: 2025.02.21 09:38:35 -06'00'

Privacy Officer, Marvis Harvey

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2025.02.22 21:35:39 -05'00'

Information System Security Officer, Joseph Facciolli

CHRISTINA LAWYER

Digitally signed by CHRISTINA LAWYER
Date: 2025.02.24 09:40:44 -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).

eGovernment Act of 2002, Pub. L. No. 107–347 § 208(b)(1)(B)(iii). (2002). Retrieved from https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

U.S. Department of Veterans Affairs. (2022, September 30). *Notice of Privacy Practices (NOPP)*. Retrieved from https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

U.S. Department of Veterans Affairs. (2024, November 08). *Privacy Act Statement*. Retrieved from https://www.va.gov/privacy-policy/#on-this-page-76

U.S. Department of Veterans Affairs. (2021, November 8). *System of Record Notice (SORN): VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records–VA (58VA21/22/28)*. Federal Register. Retrieved from https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

Veterans Benefits Administration. (2025). Privacy Impact Assessment for VBMS Exam Management (eMASS ID# 2053). U.S. Department of Veterans Affairs. Retrieved from https://department.va.gov/privacy/privacy-impact-assessments/

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)