



Privacy Impact Assessment for the VA IT System called:

DBQ Portal

Veterans Benefits Administration(VBA) Benefits, Appeals, and Memorials(BAM)

Date PIA submitted for review:

09/11/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jean-Claude Wicks	<i>jean-claude.wicks@va.gov</i>	(202)502-0084
Information System Security Officer (ISSO)	Joseph Facciolli	<i>Joseph.Facciolli@va.gov</i>	(215)983-5299
Information System Owner	Christina Lawyer	<i>Christina.Lawyer@va.gov</i>	(518)210-0581

Abstract

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

The Disability Benefits Questionnaire (DBQ) Portal fundamentally is a system where Medical Disabilities Exam Office (MDEO) contract vendors and field examiners enter Disability Benefits Questionnaires (DBQs) info and submit to Veterans Benefits Management System(VBMS).

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. *The IT system name and the name of the program office that owns the IT system.*
DBQ Portal | Benefits, Appeals, and Memorials(BAM)

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

The DBQ Portal is a system where Medical Disabilities Exam Office (MDEO) contract vendors and field examiners enter Disability Benefits Questionnaires(DBQs) info and submit to VBMS. There are two aspects of the DBQ Portal: an independent API and a comprehensive UI which will include user management, work queues, integrations with other C&P apps (Claim Evidence, Exam Management, as well as Core services such as Veteran, Claims, Contentions). The API will directly integrate with the Data Access Service (DAS) via REST API calls and the payload will be XML messages defined in an Information Exchange Package Documentation (IEPD). The system will exchange PII including Name, Birthdate, and personal identifiers such as SSN and File Number and PHI such as medical records.

C. *Indicate the ownership or control of the IT system or project.*
VA Owned and VA Operated

2. Information Collection and Sharing

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

The system is expected to store Veterans’ information over time. The number of individuals whose information is stored in the system is expected to exceed one million over time. The typical client is a Veteran who has had an examination performed.

E. *A general description of the information in the IT system and the purpose for collecting this information.*

The information in DBQ Portal are DBQ’s in the form of XML and PDF data from external systems (Compensation and Pension Record Interchange (CAPRI), MDEO vendors), they are stored for draft

status, and then produce DBQ messages containing all the information as well as a RESTful Application Program (RAP) object to be sent to DAS. DBQ's are forms that guide a physician during an exam to ensure that all the information needed to correctly rate a disabled veteran's conditions is properly recorded.

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

DBQ Portal is hosted on BIP. Benefits Integration Platform (BIP) provides a container-based application platform in VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) in which VA Benefits, Appeals, and Memorial (BAM) applications can be hosted. The platform leverages Kubernetes clusters for container management and orchestration, which allows teams to develop, scale, and deliver modern, secure, and properly segmented (from a storage, network, and compute perspective) applications in a multi-tenant environment. The AWS Virtual Private Clouds (VPCs) within BIP are sequentially peered to allow connectivity between VPCs, which supports the promotion of container images from lower VPCs to higher VPCs. The peering is essential for DevOps and Agile methodologies and is locked down to only allow container images to be mirrored between registries in each VPC. BIP also leverages a suite of Technical Reference Model (TRM) approved Commercial off-the-shelf (COTS) tools (e.g. Jenkins, SonarQube, Vault, Nexus, Consul) to help development teams deliver quickly and effectively. In addition, BIP, as a General Support Systems (GSS), will further support VA minor application tenants by constraining the controls necessary for applications hosted on the platform.

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

DBQ Portal is not operated in more than one site.

3. Legal Authority and SORN

H. A citation of the legal authority 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. (58VA21/22/28) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA - <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf> 2012 58VA21/22/28 SORN located at 2021-24372.pdf (govinfo.gov).

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?

The SORN will not require amendment or revision. The current SORN covers cloud usage and storage.

D. System Changes

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

Completion of this PIA is not expected to result in a change to business process.

- K. Whether the completion of this PIA could potentially result in technology changes
 Completion of this PIA is not expected to 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://vawww.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.

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:

- | | | |
|--|---|---|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Health Insurance | <input type="checkbox"/> Integrated Control |
| <input checked="" type="checkbox"/> Social Security | <input type="checkbox"/> Beneficiary Numbers | <input type="checkbox"/> Number (ICN) |
| Number | <input type="checkbox"/> Account numbers | <input type="checkbox"/> Military |
| <input type="checkbox"/> Date of Birth | <input type="checkbox"/> Certificate/License | <input type="checkbox"/> History/Service |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> numbers* | <input type="checkbox"/> Connection |
| <input checked="" type="checkbox"/> Personal Mailing | <input type="checkbox"/> Vehicle License Plate | <input type="checkbox"/> Next of Kin |
| Address | <input type="checkbox"/> Number | <input checked="" type="checkbox"/> Other Data Elements |
| <input checked="" type="checkbox"/> Personal Phone | <input type="checkbox"/> Internet Protocol (IP) | (list below) |
| Number(s) | <input type="checkbox"/> Address Numbers | |
| <input type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Medications | |
| <input type="checkbox"/> Personal Email | <input checked="" type="checkbox"/> Medical Records | |
| Address | <input type="checkbox"/> Race/Ethnicity | |
| <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Tax Identification | |
| Information (Name, Phone | <input type="checkbox"/> Number | |
| Number, etc. of a different | <input type="checkbox"/> Medical Record | |
| individual) | <input type="checkbox"/> Number | |
| <input type="checkbox"/> Financial Information | <input type="checkbox"/> Gender | |

Veterans – File number
 VA Contractors – Office name, contract identifier

PII Mapping of Components (Servers/Database)

DBQ Portal consists of **3** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **DBQ Portal** 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 the server names in the table. **The first table of 3.9 in the PTA should be used to answer this question.**

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VBMSUI	Yes	Yes	Veteran Info (name, address, phone, SSN, File Number) Claim and Contention Information (medical history and details related to specific issues) Document Information (File number and document metadata)	Requesting medical information from veterans.	Encryption at rest, encryption in transit. Secure Socket Layer (SSL) and mutual Transport Layer Security(TLS). All data is stored in a secured database.
VBMSEXAM	Yes	Yes	Veteran Info (name, contact info (address and phone), SSN, File Number) Claim and Contention Information (medical history and details related to specific issues)	Requesting medical information from veterans.	Encryption at rest, encryption in transit (SSL) mutual TLS. All data is stored in a secured database.

VBMSDASINTG	Yes	Yes	Veteran Info (name, address, phone, SSN, File Number) Claim and Contention Information (medical history and details related to specific issues)	Requesting medical information from veterans.	Encryption at rest, encryption in transit (SSL) mutual TLS. All data is stored in a secured database.
-------------	-----	-----	--	---	---

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 information is collected by Medical Disabilities Exam Office (MDEO) contract vendors and field examiners who perform examinations on individuals and enter Disability Benefits Questionnaires (DBQs) information and submit to VBMS.

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.

The DBQ forms must be filled out and submitted by the MDEO contract vendors and field examiners and submitted to VBMS, through DAS.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The system does not create information.

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?

The information is collected from DAS. Connections will be made incoming to the service via REST from MDEO vendors, and CAPRI systems using secured Secure Socket Layer/Transport Layer Security (SSL/TLS) encryption.

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

The 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.

The information is checked for accuracy by the DBQ Validation Tool. This application validates the syntax and the semantics of the DBQ data.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

No commercial aggregator is used in this process. The associated data undergoes basic business logic validation, such as confirming it is of the proper format or matches an approved value, when applicable. The files and associated data are confirmed by users performing claim processing.

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

The System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (November 8, 2021). This SORN can be found online at <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf> 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 IRS memo FD698-FED-AWS GovCloud-L-031020 For the Secure Enclave, legal authority for Federal Tax Information, to include identity information, be shared between Department of the Treasury/IRS and VA is codified in Internal Revenue Code §6103(l)(7), with identity information codified in §6103(b)(6). The ISA/MOU governing the information exchange between IRS and VA is codified in DART 52.As for the Veteran eFolder in Virtual VA (VVA)within which FTI documents will be available, the Secretary of Veterans Affairs established guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 8111(38 U.S.C.5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense HealthCare Resources," and the authorities contained under Title 10, United States Code, section 1104 (10U.S.C.51104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the “Economy Act.” These guidelines assist in the implementation of these statutes. https://www.oprm.va.gov/docs/Current_SORN_List_10_19_2021.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: PII information poses a moderate risk, as determined by the privacy officer. This is if PII is leaked or shared outside of the secure enclave with AWS.

Mitigation: Data is stored in a secure enclave within AWS. Access to information is protected by industry standard authentication and authorization protocols.

Section 2. Uses of the Information

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

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

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

Name: Veteran identification

File Number: used as veteran identifier

Social Security Number: Verify Veteran's identity and as a file number for the Veteran

Address: used to send correspondence and used to identify field examiner proximity

Phone number: Used for contacting the Veteran

Medical Records: used as medical information for field examiners

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 DBQ Validation Tool validates the syntax and semantics of the DBQ data.

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.

DBQ Portal does not create or make available new or previously unutilized information about an individual.

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?

Secure Socket Layer (SSL)/Transport Layer Security (TLS) encryption 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?

Data is hosted in Amazon Web Services(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 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?

Users must be registered within VA systems to access, and user must be authorized based on user roles to access all information.

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. 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?

Every individual accessing, processing, and in contact with PII is responsible for assuring that the data is and remains secure.

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*

Information is not retained by DBQ Portal. Relevant data will be stored in the Veteran's eFolder within VBMS Core.

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.*

DBQ Portal collects but does not retain information.

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. 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.

VA follows its Record Control Schedule and the NARA General Records Schedule (GRS) for records retention and disposition. Records Control Schedule VB-1, Part 1 Section XIII, Item 13-052.100

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.

https://www.va.gov/vapubs/search_action.cfm?dType=1

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.

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

Mitigation: Controlled access to the data is maintained. Only those personnel required by job assignment have access to the data. Each employee with access to the data is required to attend data privacy train.

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

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Data Access Service (DAS)	Used as a gateway to pass messages from external vendors to internal VA systems	Messages and Data as described in the IEPD which includes Veteran, claim, contention, medical instruction, and medical history.	REST (POST) via 2 way SSL

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 SPI is that this data may be disclosed to individuals who do not require access, which would increase the risk of the information being misused.

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

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

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
N/A				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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 the VA.

Mitigation: Not Applicable as there is no sharing of information outside of the VA.

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.

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). This SORN can be found online at <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

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

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). This SORN can be found online at <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

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.

Notice for the collection of Personally Identifiable Information is outlined in SORN 58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

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.

Responding to information collection is voluntary; however, if information is not provided; benefits may be denied.

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

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

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

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (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 Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Follow the format below:

Privacy Risk: A risk exists that members of the public may not know how many systems their information traverses over the Veterans Affairs network.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists including the Privacy Act statement and a System of Record Notice.

Section 7. Access, Redress, and Correction

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

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

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.***

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

7.1b 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 Privacy Act.

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

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

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

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

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to

be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.5

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

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

Individuals are notified of procedures for correcting their information via SORN published in the Federal Register (SORN 58VA21/22/286 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA).

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 ensure data accuracy.***

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

Procedures for redress and amendment are outlined in the System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records –VA” 58VA21/22/28 (November 8, 2021). This SORN can be found online at <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Section 8. Technical Access and Security

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

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

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.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring are performed through the use of the VA's Talent Management System (TMS), the System Owner will then need to review and approve access to the system.

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?

Users from outside the VA do not 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.

Users must be registered in CSUM (Common Security User Management), a VA internal application. Access to information is based on application user roles for access to the information. For example,

Veteran Service employees who need to track the fulfillment of medical information related to a claim for benefits.

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.

There is a Benefits Integrated Platform (BIP) NDA in place. It covers all personnel working on DBQ Portal. The DBQ Portal development team is comprised of VA personnel and contractors. Access to DBQ Portal is required for system administrators and developers for day-to-day maintenance of the systems and networks. Review of access to DBQ Portal is performed on a quarterly basis by the Information System Owner (ISO) and the security engineer. Clearance is required for each person accessing the system. Contracts are reviewed annually by the Contracting Officer's Representative (COR). VA OIT provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems, or VA sensitive information as part of initial training for new users, when required by system changes, and annually thereafter.

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

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

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

8.4 Has Authorization and Accreditation (A&A) been completed for the system? No

8.4a If Yes, provide:

1. *The Security Plan Status:* Please provide response here
2. *The System Security Plan Status Date:* Please provide response here
3. *The Authorization Status:* Please provide response here
4. *The Authorization Date:* Please provide response here
5. *The Authorization Termination Date:* Please provide response here
6. *The Risk Review Completion Date:* Please provide response here
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Please provide response here

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**.

Currently In Process. Initial Operating Capability (IOC) date is 12/15/23.

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)

DBQ Portal utilizes the VA Enterprise Cloud (VAEC) and is FedRAMP approved operating on a Software as a Service model.

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.

N/A

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.

N/A

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.

N/A

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).

N/A

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

ID	Privacy Controls
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.

Privacy Officer, Jean-Claude Wicks

Information System Security Officer, Joseph Faccioli

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).

The System of record Notice SORN 58VA21/22/28 86FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA Pub Date 11/8/2021

<https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

HELPFUL LINKS:

Record Control Schedules:

<https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

<https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf>

National Archives (Federal Records Management):

<https://www.archives.gov/records-mgmt/grs>

VHA Publications:

<https://www.va.gov/vhapublications/publications.cfm?Pub=2>

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](#)