Privacy Impact Assessment for the VA IT System called:

Quality Assurance (VQA) (QAWeb)

Veterans Benefits Administration
The Veterans Rehabilitation and Employment (VR&E)

Date PIA submitted for review:

07/25/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Chiquita Dixson	Chiquita.Dixson@va.gov	202- 632-8923
Information System Security Officer (ISSO)	Derrick Martinez	Derrick.Martinez@va.gov	505-346-4836
Information System Owner	Dan Nguyen	Dan.Nguyen@va.com	708-438-5371

Abstract

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

The Veterans Rehabilitation and Employment (VR&E) Quality Assurance (QA) (QAWeb) system is used to track the quality of VR&E business processes. It contains information about how many Veterans' cases were handled correctly, how many errors were made, which forms were processed accurately. VQA reviewers analyze the outcome of cases and use the VQA system to record where errors were made.

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.*
The Veterans Rehabilitation and Employment (VR&E) Quality Assurance (VQA) system is used to track the quality of VR&E business processes. It contains information about how many Veterans' cases were handled correctly, how many errors were made, which forms were processed accurately. VQA reviewers analyze the outcome of cases and use the VQA system to record where errors were made.

B. *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
The Veterans Rehabilitation and Employment (VR&E) Quality Assurance (VQA) system is a Veterans Benefit Administration (VBA) Intranet application that captures the results of both national and local case reviews for Entitlement Determination, Rehabilitation Planning, Rehabilitation Services Delivery, Outcomes Rehabilitation, Outcomes Discontinued, and Educational or Vocational Counseling. This program facilitates detailed analysis of case review results. The application is the core quality assessment tool supporting VR&E services.

C. *Indicate the ownership or control of the IT system or project.*
The VR&E VQA system is used to track the quality of VR&E business processes. It contains information about how many Veterans' cases were handled correctly, how many errors were made, which forms were processed accurately. Approximately 40,000 records are stored from an application, depending on the information required, some data collection is mandatory while others are voluntary. Failure to provide information may result in denial of access to the health care system. Veterans may not decline or request their information not be included as part to determine eligibility and entitlement for VA compensation and pension benefits. Veterans are notified in order to have full entitlement and be eligible for benefits. VQA reviewers analyze the outcome of cases and use the VQA system to record where errors were made. This helps VR&E management improve their business processes.

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 VR&E VQA system is used to track the quality of VR&E business processes. It contains information about how many Veterans' cases were handled correctly, how many errors were made, which forms were processed accurately. Approximately 40,000 records are stored from an application, depending on the information required, some data collection is mandatory while others are voluntary. Failure to provide information may result in denial of access to the health care system. Veterans may not decline or request their information not be included as part to determine eligibility and entitlement for VA compensation and pension benefits. Veterans are notified in order to have full entitlement and be eligible for benefits. VQA reviewers analyze the outcome of cases and use the VQA system to record where errors were made. This helps VR&E management improve their business processes.

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

The VQA system contains NO information from the Veterans' case files, only information about whether the file contained errors. Redundancy and the reporting infrastructure, serves data to thousands of users VBA wide via a Web interface. It is important to understand how Personally Identifiable Information (PII) is used within the VR&E VQA system. It is used only to identify the Veterans whose cases are being reviewed. No information, PII or otherwise, is collected directly from a Veteran by any means. Name and case/SSN numbers are randomly selected by Performance Analysis and Integrity (PA&I) and the Data Warehouse. Those names and numbers are reviewed, and then transferred into the VQA system. The paper case records are reviewed, and then number and type of errors for each case are entered into the VQA system. No PII of any type is transferred from the paper case record into the VQA system. The VQA system contains only the name and case/SSN number of the Veteran, the name of the VR&E counselor who provided service to the Veteran, the name of the VQA reviewer who reviewed the case and the errors (if any) that the reviewer found. The VR&E VQA system is a VBA Intranet application that captures the results of both national and local case reviews for entitlement determination, rehabilitation planning, rehabilitation services delivery, outcomes rehabilitation, outcomes discontinued, and educational or vocational counseling. This program facilitates detailed analysis of case review results. The application is the core quality assessment tool supporting VR&E services. Users of the system are VR&E central office, officers, counselors, and Quality Assurance staff; all users are internal to VBA.

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

The VR&E VQA system is used to track the quality of VR&E business processes. It contains information about how many Veterans' cases were handled correctly, how many errors were made, which forms were processed accurately. Approximately 40,000 records are stored from an application, depending on the information required, some data collection is mandatory while others are voluntary. Failure to provide information may result in denial of access to the health care system. Veterans may not decline or request their information not be included as part to determine eligibility and entitlement for VA compensation and pension benefits. Veterans are notified in order to have full entitlement and be eligible for benefits. VQA reviewers analyze the outcome of cases and use the VQA system to record where errors were made. This helps VR&E management improve their business processes.

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.*
This system is hosted by the Austin Information Technology Center (AITC) on an Isolated Customer LAN (ICL) in Austin, TX.

3. Legal Authority and SORN

H. *A citation of the legal authority to operate the IT system.*
The Legal Authority for Operating this system is: SORN- *58VA21/22/28 VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA.*
Title 38, United States Code (U.S.C.), Sections 501 (a), 501
(b), 304, 1705, 1710, 1722, and 5317.

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?*
N/A

D. System Changes

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

K. *Whether the completion of this PIA could potentially result in technology changes*
N/A

Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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

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

- Name of the VR&E counselor who provided service to the Veteran
- Name of the QA reviewer who reviewed the case, and the errors (if any) that the reviewer found.
- Case Number

The VQA (QAWeb) system contains only the name and case/SSN number of the Veteran, the name of the VR&E counselor who provided service to the Veteran, the name of the VQA reviewer who reviewed the case, and the errors (if any) that the reviewer found.

PII Mapping of Components (Servers/Database)

Quality Assurance (VQA) (QAWeb) consists of **1** key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Quality Assurance (VQA) (QAWeb)** 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
VBA Data Management Warehouse (VD2)	**Yes**	**No**	• Name • Case Number • SSN Number	PII in the name and case/SSN number of the Veteran whose case was reviewed.	Limited number of admin users. All administrative users undergo mandated annual security and privacy training

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?

No information, PII or otherwise, is collected directly from a Veteran by any means. Name and case/SSN numbers are randomly selected by Performance Analysis and Integrity (PA&I) and the Veteran Benefit Administration (VBA) Data Warehouse. Those names and numbers are reviewed, and then transferred into the VQA system. The information is collected for reviews from the VBA Warehouse database.

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.

N/A

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

N/A

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 only PII is the name and Case/SSN number of the Veteran whose case was reviewed. This system is not the master or original source of this info. The data is collected from PA&I and the data warehouse. The QAWeb system contains only the name and case/SSN number of the Veteran, the name of the VR&E counselor who provided service to the Veteran, the name of the QAWeb reviewer who reviewed the case, and the errors (if any) that the reviewer found. The information is transferred via internal Intranet.

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 QAWeb data is not collected via 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 purpose of the VR&E VQA system is used to track the quality of VR&E business processes. It contains information about how many Veterans' cases were handled correctly, how many errors were made, which forms were processed accurately. VQA reviewers analyze the outcome of cases and use the VQA system to record where errors were made. This helps VR&E management improve their business processes.

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.

N/A

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 Legal Authority for Operating this system is: Title 38, United States Code (U.S.C.), Sections 501 (a), 501
(b), 304, 1705, 1710, 1722, and 5317.
SORN- *58VA21/22/28 VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA.*

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: VQA collects Personally Identifiable Information (PII). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: VQA is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA can better protect the individual's information.

VQA receives the information via a secured internal Intranet and no external exposure results from this connection.

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's Identification – Internal
Social Security Number: Used to verify Veteran identity and as a file number for Veteran – Internal
The name of the VR&E counselor who provided service to the Veteran: For records purpose-Internal
The name of the QA reviewer who reviewed the case: For records purposes – Internal
The errors (if any) that the reviewer found: For records and reference purposes - Internal
Case number: Used to verify Veterans whose case was reviewed. - Internal

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 Veterans Rehabilitation and Employment (VR&E) Quality Assurance (VQA) system is a Veterans Benefit Administration (VBA) Intranet application that captures the results of both national and local case reviews for Entitlement Determination, Rehabilitation Planning, Rehabilitation Services Delivery, Outcomes Rehabilitation, Outcomes Discontinued, and Educational or Vocational Counseling. This program facilitates detailed analysis of case review results. It contains information about how many Veterans' cases were handled correctly, how many errors were made, which forms were processed accurately. QAWeb reviewers analyze the outcome of cases and use the QAWeb system to record where errors were made. This helps VR&E management improve their business processes.

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.

N/A

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?

Audit log records user identification information along with related activity information such as search type (by name, Case/SSN number of Veteran), search parameters, and veteran identification data. Veterans' identification data is not the master or original source of this information. QAWeb is a pass-through application.

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

The only PII is the name and case/SSN number of the Veteran whose case was reviewed. This system is not the master or original source of this info. The data is collected from PA&I and the data warehouse. The QAWeb system contains only the name and case/SSN number of the Veteran, the name of the VR&E counselor who provided service to the Veteran, the name of the QAWeb reviewer who reviewed the case, and the errors (if any) that the reviewer found. The information is transferred via secured internal Intranet.

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

There is no PHI data in QAWeb. QAWeb application code is periodically scanned and security vulnerabilities are fixed. Server infrastructure is regularly patched with updates per VA standards. These practices ensure proper security procedures are in place. QAWeb application is internal facing and users outside the VA firewall cannot access it. Supervisors requesting access for their employees are responsible to ensure sensitive information is appropriately safeguarded and used responsibly.

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?

The SORN defines the information collected from Veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a Veteran's benefits, such as compensation or education. SORN: 58VA21, 58VA22, 55VA28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. The security controls for the VQA application cover 17 security areas with regards to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity.

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

Yes these processes are documented in eMass.

2.4c Does access require manager approval?

Yes the manager approvals are required for QAWeb access.

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

N/A

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

The VA Manager is responsible for assuring safeguards are implemented for the PII.

Section 3. Retention of Information

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

3.1 What information is retained?

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

Name

Social Security Number
The name of the VR&E counselor who provided service to the Veteran
The name of the VQA reviewer who reviewed the case
The errors (if any) that the reviewer found

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.*

Records are maintained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States. Records from this system will be disposed of 6 years after a user's account becomes inactive. Routine records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes. These retention and disposal statements are pursuant to 58VA21/22/28 - Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA

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

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

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

The VA procedures for eliminating data are available from the VBA Records Control Schedule, VB-1. The retention schedule has been approved by the National Archives and Records Administration (NARA). VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc www.benefits.va.gov/warms/docs/admin20/rcs/part2/vb-1partii.doc as authorized by NARA. These retention and disposal statements are pursuant to 58VA21/22/28 - Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA https://www.benefits.va.gov/WARMS

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

The VA procedures for eliminating data are available from the VBA Records Control Schedule, VB-1.The retention schedule has been approved by the National Archives and Records Administration(NARA). VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc www.benefits.va.gov/warms/docs/admin20/rcs/part2/vb-1partii.doc as authorized by NARA. These retention and disposal statements are pursuant to 58VA21/22/28 - Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA

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.

Records/digital information will be eliminated following the sanitization procedures in VA 6300.1 HB RECORDS MANAGEMENT PROCEDURES and VA 6500.1 Electronic Media Sanitization. Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization.
Disposition of Printed Data:
Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

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.

VQA uses test data in a testing environment for testing the system. VA Handbook 6500 mandates that Systems under development should not process “live data” or do any real processing in which true business decisions will be based. Test data that is de-identified should be used to test systems and develop systems that have not yet undergone security A&A. Furthermore, systems that are in development (pilot, proof-of-concept, or prototype) should not be attached to VA networks without first being assessed and authorized. Additionally, VA wide Directive 6511 describes the responsibilities, requirements and procedures for eliminating PII or information exempt from release under FOIA from presentations that may be seen by non-VA parties. This Directive includes guidance for conducting privacy reviews of presentations, and the criteria for when presenters must self-certify that their presentations are devoid of PII or information exempt from release under FOIA.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

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

Mitigation: To mitigate the risk posed by information retention, VQA adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individual's information is carefully
disposed of by the determined method as described in General Records Schedule 10-1.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VBA Data Management	VD2 is the main database for VQA to perform long-term statistical analysis of quality trends	Name of the VR&E counselor who provided service to the Veteran Name of the QA reviewer who reviewed the case, and the errors (if any) that the reviewer found.	VA internal Intranet.
Performance Analysis and Integrity (PA&I)	Perform long-term statistical analysis of quality trends	Name and SSN/Case file number	VA internal Intranet.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

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

Mitigation: The principle of need-to-know is strictly adhered to by the VQA personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System	*List the purpose of information*	*List the specific PII/PHI data elements that are processed*	*List the legal authority,*	*List the method of transmission*

information is shared/received with	***being shared / received / transmitted with the specified program office or IT system***	***(shared/received/transmitted) with the Program or IT system***	***binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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:

<u>Privacy Risk:</u> The privacy risk associated with maintaining PII is that sharing data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

<u>Mitigation:</u> Besides the fact that VQA does not share information externally. The principle of need-to know is strictly adhered to by VQA personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system.

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.

1) The SORN defines the information collected from Veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a Veteran's benefits, such as compensation or education. Notice of Amendment of System of Records, SORN:58VA21/22/28 VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

This Privacy Impact Assessment (PIA) also serves as notice of the VQA System. As required by the Government Act of 2002, Pub. L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." 2021-24372.pdf (govinfo.gov)

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

N/A

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.

While QAWeb does not collect information directly from the Veteran but instead from the source application of VD2, depending on the information required, some data collection is mandatory while others are voluntary.

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.

While QAWeb does not collect information directly from the Veteran but instead from the source application of VD2, depending on the information required, some data collection is mandatory while others are voluntary. Failure to provide information may result in denial of access to the health care system. Veterans may not decline or request their information not be included as part to determine eligibility and entitlement for VA compensation and pension benefits. Veterans are notified in order to have full entitlement and be eligible for benefits.

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

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

Any right to consent to particular uses of the information would be handled by the source systems that collect the information from the Veteran and feed VQA with information.
The source system is: VD2.

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: There is a risk that members of the public may not know that the VQA system exists within the Department of Veterans Affairs.

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

Section 7. Access, Redress, and Correction

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

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

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.***

Individuals wishing to obtain more information about access, redress and record correction of VQA should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) 58VA21/22/28 VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA.https://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf
2021-24372.pdf (govinfo.gov)

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).

N/A

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.

N/A

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 wishing to obtain more information about access, redress and record correction of VQA should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice(SORN) 58VA21/22/28 VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. Department of Veterans Affairs, Federal Benefits for Veterans and Dependents (80D), 810 Vermont Ave. NW., Washington, DC 20420.https://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf [2021-24372.pdf (govinfo.gov)]()

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

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

Individuals are not notified if there is missing or inaccurate information in their record. An individual who wishes to determine whether a record is being maintained under his or her name in the VQA system or wishes to determine the contents of such records should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) 58VA21/22/28 VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. Department of Veterans Affairs, Federal Benefits for Veterans and Dependents (80D), 810 Vermont Ave. NW., Washington, DC 20420.https://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf

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

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

Individual wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records should contact the Department of Veteran's Affairs Regional Office at 1-800-827-1000. Veterans Services Representatives are available from 7:00 AM to 7:00 PM (Eastern Time), Monday thru Friday, except for federal holidays. For more information – see https://department.va.gov/privacy

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals 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.

A small number of QAWeb employees (up to 5) will have administrative access to the system. This access will be used to perform maintenance, troubleshooting, and updates to QAWeb. System administrators will not be able to change information that users have entered. No one from other agencies will have system access. We limit the number of administrative users having access to QAWeb. All administrative users undergo mandated annual training, including privacy and HIPAA focused training and VA privacy and information security awareness training.

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?

N/A

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.

N/A

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

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

Yes, contractors will have access to the system. The access is verified through VA VR&E personnel before access is granted to any contractor. Contracts are reviewed annually at a minimum. 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 TMS. All contractors are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI).

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

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

Users are required to complete information system security training activities including annual security awareness training and specific information system security training. The training records are retained for7 years. This documentation and monitoring are performed using Talent Management System (TMS).

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* June 8, 2023
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* June 10, 2022
5. *The Authorization Termination Date:* June 09, 2025
6. *The Risk Review Completion Date:* September 21, 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

The VQA application was granted a full ATO on June 8, 2022, for 3 years. The FIPS 199 classification of the system is Moderate. The current ATO was submitted on June 10, 2022 in eMass and will not expire until June 9, 2025.

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.***

Please provide response here

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)*

No

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
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.

CHIQUITA DIXSON

Digitally signed by CHIQUITA DIXSON
Date: 2023.08.11 14:33:19 -04'00'

Privacy Officer, Chiquita Dixson

Derrick J Martinez 378778

Digitally signed by Derrick J Martinez 378778
Date: 2023.08.11 14:23:37 -06'00'

Information System Security Officer, Derrick Martinez

DAN NGUYEN

Digitally signed by DAN NGUYEN
Date: 2023.08.14 05:50:04 -05'00'

Information System Owner, Dan Nguyen

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).

System of Records Notice (SORN)

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

HELPFUL LINKS:

VA Privacy

https://department.va.gov/privacy

Web Automated Reference Material System

https://www.benefits.va.gov/WARMS

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