Privacy Impact Assessment for the VA IT System called:

Performance Analysis and Integrity (PA&I) Business Intelligence (VD3)

Performance Analysis and Integrity Veterans Benefits Administration

Date PIA submitted for review:

09/07/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Chiquita Dixon	Chiquita.Dixson@va.gov	202-632-8923
Information System Security Officer (ISSO)	Ahmed Tamer	Tamer.Ahmed@va.gov	202-461-9306
Information System Owner	Benjamina Shofner	jami.shofner@va.gov	512-820-4810

Abstract

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

The Performance Analysis and Integrity (PA&I) Business Intelligence (VD3) is a software environment that allows VA authorized users the ability to analyze and share data extracts from the Veterans Benefit Administration (VBA) Data Management Warehouse (VD2) and the Statistical Analysis System (SAS).

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Performance Analysis and Integrity (PA&I) Business Intelligence owned by the office of Performance Analysis & Intelligence is a software environment that allows VA authorized users the ability to analyze and share data extracts from the Veterans Benefit Administration (VBA) Data Management Warehouse (VD2) and the Statistical Analysis System (SAS). VBA Data Management Warehouse is the central repository of all Benefits related data, receiving data input from multiple

VA data sources and providing reporting, analysis, and payment data to various organizations throughout the VA and both the Executive and Legislative branches.

The VD3 Server software licenses allow for users to analyze, visualize and share data. The Tableau Environment serves as a VBA-wide application providing interfaces which are the common services that the Tableau uses in order to generate reports to business users. These reports provide data and information in support of Veteran benefits. Only users with VA accounts are allowed access to any information. The Tableau Server software provides controlled access to data and a platform for enterprise-wide sharing of analyses. Tableau Server acts as the distribution hub for managed data extracts as well as a collaboration point for sharing analyses produced by Tableau Desktop based on the data extracts. Users with the Desktop Pro licenses can connect to these data extracts based on roles assigned to them, allowing for easy administration of security and data governance. From Tableau Server, users can then share reports/visualization/dashboards via the web including websites, mobile devices, and portals such as SharePoint. Tableau reports are developed using data from VD2 (Data Management Warehouse and SAS via Tableau Desktop. In addition to that some users use Tableau Professional Desktop which runs as an independent tool to analyze, visualize, and share data, however, it requires Tableau Server to publish it on web, if needed.

The VBA Tableau Server is installed on Windows systems in Austin Information Technology Center (AITC).

Only user account records are retained in the Tableau application. The information Tableau uses is derived from VD2 and SAS in the form of graphics and reports developed by Tableau but not stored in the application. User inquiries (extracted data from VD2) are displayed by VD3 in a dashboard type report. The information is saved in VD2 and is exportable to other storage locations. The extracted report is not stored by the VD3 system. Approximately 2,000 user account records are retained by VD3. This application does not use cloud technology.

Legal authority for maintaining the system is Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55.

•SORN: The authority for VBA to share data for the purpose indicated under the Privacy Act is Routine Use #60 of VBA's System of Records, "Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA" (58VA21/22/28), published at 74 FR 29275, June 19, 2009, last amended at 86 Fr 61858, November 8,2021

•VBA will not disclose medical information in claims files that is protected by 38 U.S.C.§ 7332, relating to drug abuse, alcoholism, or infection with the Human Immunodeficiency Virus (HIV) or sickle cell anemia, without the prior written authorization from the Veteran or his/her authorized representative.8

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 Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☒ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integration Control Number (ICN)
☐Military History/Service Connection
☐ Next of Kin
☒ Other Unique Identifying Information (list below)

VD3 also collects and processes Benefits/Claims, Eligibility Information, Payee Number, Type of Benefits.

PII Mapping of Components

VD3 consists of 2 key components – data transfer, data analysis/report generation. Each component has been analyzed to determine if any elements of that component collect PII. None of the PII data is collected from primary sources or retained, only used in analysis and report generation. None of the analyses or reports are retained

PII Mapped to Components

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.

PII Mapped to Components

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
Veterans Benefits Administration (VBA) Data Management Warehouse (VD2)	Yes	Yes	All PII/PHI listed in 1.1	Benefits claims	Safeguards are multi-level, from those native to the Tableau environment to those mandated by VA Policy. Please refer to section 2.3 for detailed safeguards

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

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

VD3 data sources are from VBA Data Management Warehouse (VD2) and the Statistical Analysis System (SAS), VD3 Server acts as the distribution hub for managed data extracts as well as a collaboration point for sharing analyses produced by Tableau Desktop based on the data extracts of the above-mentioned systems. The analyses and reports are not retained on the VD3 system.

1.3 How is the information collected?

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

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

Tableau gathers data from VD2 and SAS electronically; Tableau system user information is electronically collected from the Active Directory.

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

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

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

VD3 does not collect data from primary sources, only from the VD2 data warehouse and SAS. SAS also obtains its initial data from the VD2 data warehouse. When transmitted to the VD3 system, the data is validated for accuracy only against the data in the VD2 data warehouse.

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) Veterans Information Solution (VIS)—
VA has been rescinded and is no longer in effect.
The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources." and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, 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.
•VBA will not disclose medical information in claims files that is protected by 38 U.S.C.§ 7332, relating to drug abuse, alcoholism, or
infection with the Human Immunodeficiency Virus (HIV) or sickle cell anemia,
without the prior written authorization from the Veteran or his/her
authorized representative.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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:
<u>Privacy Risk:</u> VD3 visually disseminates Personally Identifiable Information (PII) and other highly delicate information possibly including Personal Health Information (PHI). If this

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

Mitigation: The source systems used by Tableau are owned/managed by the Department of Veterans Affairs. The VA is careful to only collect the information necessary to accomplish the VA mission. By only disseminating the minimum necessary information with Tableau, the VA can better protect the individual's information.

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.

The VD3 software environment is to provide expanded data analysis capability in supporting VBA benefits administration services to veterans. Dependent upon search criteria entered the results may vary. The uses described below are generalized as the use of the disseminated data may vary greatly upon the role and job classification of the user requesting the report.
Reports may disseminate:

- Name – used as veteran identifier and correspondence –internal
- Social Security Number (SSN) – used as veteran identifier–internal
- Date of Birth (DOB) – used as veteran identifier–internal
- Mailing Address - correspondence –internal
- Zip Code – part of mailing address – statistical reporting –internal
- Phone Number(s) - correspondence–internal
- Email Address- communication- internal
- Financial Account Information – eligibility – benefits administration–internal
- Previous Medical Records – eligibility – benefits administration–internal
- Benefits/Claims Information – benefits administration–internal
- Eligibility Information – benefits administration–internal
- Payee Number – benefits administration–internal
- Type of Benefits – benefits administration – statistical reporting–internal

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The VD3 software environment was designed for data analysis. Tableau is the tool for data analysis. Data produced is varied to include reports/visualization/dashboards. Results can vary from one veteran to statistics of an entire program office or full scope on the entire VBA.

2.3 How is the information in the system secured?

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

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

Report data is transmitted securely using Secure Hypertext. Transfer Protocol (HTTPS)/Single Socket Layer (SSL) or Transport Layer Security (TLS) a standard security technology for establishing an encrypted link between a web server and a browser. The system uses these safeguards in accordance with OMB M-06-15 while in possession of the information, however it does not retain this information and safeguarding the information where it is retained in respect to OMB-M-06-15 is the responsibility of those retaining systems.

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

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Add answer here:

The System of Record Notice(s) (SORNs) that apply to this system define 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 eligibility and benefits, such as compensation or education.
" 58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

The types of controls that are in place for VD3 are as follows: The minimum-security requirements for Tableau's high impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related 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. Our facilities employ all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. Users are trained how to handle sensitive information by taking VA Privacy and security awareness training and reading and attesting they understand the VA Rules of Behavior. Additionally, VD3 users who have access to PHI must also take VA HIPPA focused training. VA Privacy and Information Security Awareness training must be accomplished before gaining access to the Tableau application and annual basis thereafter. Role based access limits the scope and access the users have to information in Tableau.

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

Only VA system user information is stored in VD3.
•Name – VA employee (system user)
•Work Phone
•Station Number
•Job Title
•Organization/Contractor Company Name
•Organization/Contractor Company Address

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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

VA Records Control Schedule (RCS) 10-1- January 2016 States:
3.System Access Records.
These records are created as part of the user identification and authorization process to gain access to systems. The information system follows the VA RCS guidelines. Records are used to monitor inappropriate systems access by users. Includes records such as:
•User profiles
•Log-in files
•Password files
•Audit trail files and extracts
•System usage files
•Cost-back files used to assess charges for system use
EXCLUSION 1: excludes records relating to electronic signatures.

EXCLUSION 2: does not include monitoring for agency mission activities such as law enforcement.

a. Systems not requiring special accountability for access. These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users. Temporary; destroy when business use ceases. (DAA-GRS-2013-0006-0003, item 030)
b. Systems requiring special accountability for access. These are user identification records associated with systems which are highly sensitive and potentially vulnerable. Temporary; destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. (DAA-GRS-2013-0006-0004, item 31)

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

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

VA Records Control Schedule (RCS) 10-1is approved by NARA.

3.4 What are the procedures for the elimination of SPI?

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

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

VD3 itself does not use PII for research, testing, or training. Reports or analyses created by VD3 may be used by other groups for those purposes. The reports and analyses created and presented by VD3 are only disseminated to appropriate vetted destinations, as detailed in 1.7 above.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that the information maintained by VD3 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, the VD3 staff adhere to the VA RCS schedule for the user data it maintains

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***
Veterans Benefits Administration (VBA) Data Management Warehouse (VD2)	VD3 extracts data from VD2 to provide reporting	Depending upon the criteria the user selects and has access to, the reports could contain (but not limited to) the following: •Name •Social Security Number (SSN) •Date of Birth (DOB)	Report data is transmitted securely using Secure Hypertext Transfer Protocol (HTTPS)/Single Socket Layer (SSL) or Transport Layer

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***
		•Mailing Address •Zip Code •Phone Number(s) •Email Address •Financial Account Information •Previous Medical Records •Benefits/Claims Information •Eligibility Information •Payee Number •Type of Benefits	Security (TLS) a standard security technology for establishing an encrypted link between a web server and a browser.

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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

Follow the format below:
<u>Privacy Risk:</u> The privacy risk associated with maintaining and internal agency transfer of PII is that while sharing data within the Department of Veterans' Affairs the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

<u>Mitigation:</u> The principle of need-to-know is strictly adhered to by VD3 personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within. Additionally, VD3 only retains the minimum amount of information (VA user data) to authenticate the users of VD3. Role based access is implemented to ensure that the VD3 user only has access to the information they are authorized to see.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

VD3 does not currently share data external of the VA boundary.

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: VD3 does not share data externally thus the risk of misuse or compromise is minimal externally.

Mitigation: VD3 is protecting the minimal stored PII within the VA boundary using all appropriate security controls in accordance with VA policy. No data is shared externally. Therefore, the mitigation to the minimal risk of compromise is protected by the implementation of the security controls listed in VA 6500 Handbook.

Section 6. Notice

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

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

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

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

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

This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

VD3 only collects data from VA users via form 9957 which contains the following:
PRIVACY ACT STATEMENT: The information is solicited under authority of Title 38, United States Code and Executive Order 9397 and is necessary to accomplish the action requested by the requester, including establishing, modifying or deleting a Customer Account. Furnishing the information on this form is voluntary; however, if the information is not furnished, we will be unable to take further action on your request. NOTE: Information from this form is used to establish VA Accounts or to grant access to VA resources.
The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

1.The System of Record Notice (SORN) are as follows:
a. SORN 58VA21/22/28 –"Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA.". The Amended SORN can be found online at:
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

2.This Privacy Impact Assessment (PIA) also serves as notice of the VD3 system required by the Government Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii).

a. 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." VA PIAs can be found athttp://www.oprm.va.gov/privacy/pia.aspx

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

VD3 only retains information on VA Information Technology (IT) system users that requested access to the system. Users do have the right to decline to provide information when applying using a VA form 9957. Furnishing the information on that form is voluntary; however, if the information is not furnished, system administrators will be unable to take further action on the request. VD3 reports are generated from the VD2 system/application and the right to decline would be based upon the sources feeding VD2.

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

System users are required to furnish all the information on the system request form. If the information is not furnished, system administrators will not be able to take further action on the request. VD3 reports are generated from the VD2 system/application and the right to consent to users would be based upon the sources feeding 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.

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 VD3 system exists within the Department of Veterans Affairs. Additionally, there is a minimal risk that the individual may not receive notice of information collection and use.

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 System of Record Notice.

Section 7. Access, Redress, and Correction

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

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

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

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

As published in the SORN, individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office (www.va.gov)

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.

As published in the SORN, individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office

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.

As published in the SORN, individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

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

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that information provided by or about the individual is incorrect and will become part of the data file. There is also 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 files stored on the VD3 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 files.

Section 8. Technical Access and Security

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

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

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

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

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

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

After completing onboarding, training and background checks to gain initial computer access, users requesting access to the VD3 system is controlled by a formal access control process using the VA 9957 form with several layers of approval starting with the employee/contractor's supervisor/contracting officer's representative (COR).
Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.
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 all personnel. This documentation and monitoring is performed through the use of VA's Talent Management System (TMS).

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.

VA contract employee access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access 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 TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

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 which all personnel must complete via the VA’s Talent Management System (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 system. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

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

If Yes, provide:

1. *The Security Plan Status* - 06-Jul-2022
2. *The Security Plan Status Date* - 04-Oct-2022
3. *The Authorization Status* – One-year ATO granted
4. *The Authorization Date*- 03-Nov-2021
5. *The Authorization Termination Date* - 03-Nov-2022
6. *The Risk Review Completion Date* – 8-2-2022
7. *The FIPS 199 classification of the system* - MODERATE

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

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

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).

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.

NO, the system does not use cloud technology.

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)

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).

The system does not use RPA

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
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 126558

Digitally signed by Chiquita Dixson 126558
Date: 2022.11.02 11:43:08 -04'00'

Privacy Officer, Chiquita Dixon

Tamer F. Ahmed 531244

Digitally signed by Tamer F. Ahmed 531244
Date: 2022.10.31 15:02:02 -04'00'

Information System Security Officer, Ahmed Tamer

Benjamina W. Shofner 304316

Digitally signed by Benjamina W. Shofner 304316
Date: 2022.11.02 09:56:30 -05'00'

Information System Owner, Benjamina Shofner

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).

VD3 only collects data from VA users via form 9957 which contains the following:

PRIVACY ACT STATEMENT: The information is solicited under authority of Title 38, United States Code and Executive Order 9397 and is necessary to accomplish the action requested by the requester, including establishing, modifying or deleting a Customer Account. Furnishing the information on this form is voluntary; however, if the information is not furnished, we will be unable to take further action on your request. NOTE: Information from this form is used to establish VA Accounts or to grant access to VA resources.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

1.The System of Record Notice (SORN) are as follows:

a. SORN 58VA21/22/28 –"Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA.". The Amended SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

2.This Privacy Impact Assessment (PIA) also serves as notice of the VD3 system required by the Government Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii).

a. 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." VA PIAs can be found https://www.oprm.va.gov/docs/PIA/FY21AdministrativeDataRepositoryPIAUpdated.pdf