Privacy Impact Assessment for the VA IT System called:

Salesforce- Office Finance Management (Salesforce- OFM) Applications

Veterans Benefits Administration (VBA)

Office of Financial Management

eMASS ID #1899

Date PIA submitted for review:

05/30/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jason Anderson	Jason.Anderson3@va.gov	202-570-0255
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000 x4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

Salesforce- Office Finance Management Applications (Salesforce-OFM) consists of seven separate modules. These modules serve primarily as workload management tools.

1) The first module to be included is Finance Cases – Manages inquiries submitted by users of the Enterprise Management of Payments, Workload, & Reporting for VA (eMPWR-VA) application and allows the Office of Financial Management staff to respond.
2) The second module is the Committee on Waivers and Compromises (COWC) Cases. The COWC manages requests for waivers of debts owed to the VA by veterans, dependents, and employees.
3) The third module that is included in the OFM Applications is the Accounting Policy and Reporting Division (APRD) Inquiries. The APRD manages the requests for accounting audits.
4) The fourth module is the Chapter 39Adaptive and Automotive Equipment Program (CH39AAEP) which is used to capture grant information as well as vehicles which have been modified for veterans with disabilities and payments related to the grants.
5) The fifth module is the Post Payment Workshop (PPW) which is used to track non receipt claims.
6) The sixth module is the Specially Adaptive Housing Assistive Technology Grant Program (SASHA – CH21) which captures grant and payment data approved to improve home adaptations for veterans to live independently.
7) The final module is the Budget Formulation and Execution (BRIT) which is used by Budget to manage the VBA Budget.

These modules except BRIT utilize the social security number (SSN), name and address data elements. These modules are hosted in Salesforce Government Cloud Plus -Enterprise (SFGCP-E).

Overview

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

1 General Description

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

Salesforce- Office Finance Management Applications (Salesforce- OFM) is owned and maintained by the Office of Financial Management – Fiscal Systems Division.

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

Its purpose is to serve as a workload management tool for Finance Cases (inquiries relating to the eMPWR-VA), COWC Cases (requests for waivers of debts owed to VA). By their nature, CH 39 AAEP, SASHA, PPW, COWC Cases & Finance Cases contain information about an individual and the nature of the issue for which the case was opened. OFM fulfills agency mission by ensuring any inquiry related to Veterans and their dependents have clear visibility and is on track for faster resolution, these applications provide the interface to fulfill OFM's mission for VBA.

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

The IT System name is Salesforce Government Cloud Plus -Enterprise (SFGCP-E) VA Assessing, which is owned by the Office of Information Technology (OI&T), Enterprise Program Management Office (ePMO). Salesforce is a FedRAMP approved product and has Agency level authorization to be used as Solution.

2. Information Collection and Sharing

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

Mostly owed to the migration of legacy COWC databases dating back to 1996, the number of individuals whose information is stored on the OFM Application is upwards of 450,000. These individuals include veterans, their dependents, and sometimes VA employees.

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

The information stored in Salesforce- OFM includes File Numbers, Social Security Numbers, names, addresses, phone numbers, and financial information. There are currently no integrations with other applications to share this information. No changes are anticipated as a result of this PIA.

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

The information is not shared to any other IT System. The SASHA and CH39AAEP integrate with eMPWR-VA through APIs and the SASHA and CH39AAEP data is passed. eMPWR-VA has its own PIA and PTA.

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

The system is not operated in more than one site.

3. Legal Authority and SORN

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

The following is a full list of related laws, regulations and policies and the legal authorities:

• Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
• Information from the SORN: 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E
• 5 U.S.C. 552, "Freedom of Information Act," c. 1967
• 5 U.S.C. 552a, "Privacy Act," c. 1974
• OMB Circular A-130, Appendix III, “Security of Federal Automated Information Systems”
• Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
• Federal Information Security Management Act (FISMA) of 2002
• OMB M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
• VA Directive and Handbook 6502, Privacy Program
• SORN 58VA21/22/28

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

The SORN is not being modified.

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

This will not results changes to existing business process.

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

This will not result in technology change.

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.

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements: File number in lieu of SSN is used.

PII Mapping of Components (Servers/Database)

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

Sales Force applications consists of **5** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **<Information System Name>** and the reasons for the collection of the PII are in the table below.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
Salesforce Government Cloud Plus (SFGP)	Yes	YES	SSN, Name, Address, DOB, File Number	These fields are needed to provide resolution to issues in timely manner.	Only approved individuals have access to these fields. Supervisors monitor for access requirements and submit termination request once the individual is no longer serving the role.
OFM Applic	Yes	YES	SSN, Name, Address, DOB, File Number	These fields are needed to provide resolution to issues in timely manner.	Only approved individuals have access to these fields.
OFM_Finance_Case__c	Yes	Yes	SSN, Name, Address, DOB, File Number	These fields are needed to provide resolution to issues in timely manner.	Only approved individuals have access to these fields. Supervisors monitor for access requirements and submit termination request once the individual is no longer serving the role.
OFM_Referral__c	Yes	No	SSN, Name, Address, DOB, File Number	These fields are needed to provide resolution to issues in timely manner.	Only approved individuals have access to these fields. Supervisors monitor for access requirements and submit termination request once the individual is no longer serving the role.
OFM_COWC__c	Yes	Yes	SSN, Name, Address, DOB, File Number	These fields are needed to provide resolution to issues in timely manner.	Only approved individuals have access to these fields. Supervisors monitor for access requirements and submit termination request once the individual is no longer serving the role.

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?

Information is generally input into Salesforce- OFM by users at Regional Finance Offices and Committees on Waivers and Compromises manually.
Information for the CH39AAEP and SASHA are obtained from integrations with VBMS.
Information is generally input into Salesforce-OFM by users at Hines manually for the PPW work items.

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

The sources for this information is always gleaned from other VBA applications to include the Enterprise Management of Payments, Workload, & Reporting for VA (eMPWR-VA), Share, and the Veteran Benefits Management System (VBMS).

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

For supervisors, Salesforce- OFM provides information in the form of reports which include summary statistics and performance metrics.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Information collected and maintained within Salesforce- OFM originates via manual entry or systematically from other VBA systems such as VBMS.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?
Data is collected on electronic forms where possible and transmitted from VBMS. We are not the source of forms, nor do we generate paper forms.

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 OFM Application is not automatically checked against any other source of information, nor are there regular designated checks for accuracy. The PPW items are checked against US Treasury reports and are matched by the SSN. Note that US Treasury systems use SSN for processing any type of payment transaction.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

As a course of regular business, information entered is typically routed utilized by multiple users so discrepancies have multiple opportunities to be identified and corrected.

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

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

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- E---Government Act of 2002 § 208 • Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A---130, Management of Federal Information Resources, 1996 Version Date: January 2, 2019 Page 5 of 19
- OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites
- OMB Memo M---99---18, Privacy Policies on Federal Web Sites
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

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: There is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

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

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
SSN, Name, File Number	Internal use to research details about the case to provide expedited resolution	Not directly used by any of the OFM SF applications.

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 data is strictly used for research purposes to address the inquiry submitted, no analysis on data is done using any of the analytical tools.

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.
Since these FIRE and COWC facilitates inquires, if new information is available, the end user submits a new inquiry and the old inquiry is closed.
CH39AAEP, SASHA and PPW facilitates new records and new records are accessible to Government employees with access to the applications for use in research, facilitating and processing financial transactions.

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?
The data at rest is protected by ensuring only approved users have access to view the inquiry details.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
Salesforce- OFM uses Salesforce built in encryption process for SSN field and other PII fields, thereby security is implemented in the design itself.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
Salesforce- OFM has security built in design and development of this application. For Operational purposes, only authorized and approved users get access to the application to perform actions based on their role, therefore role-based separation of duties is implemented. SF apps were designed, developed, deployed, and is operated and maintained within the requirements of OMB Memoranda M-06-15 Safeguarding Personally Identifiable Information and M-06-16 Protection of Sensitive Agency Information. Specifically, the VA has designated the Deputy CIO as the Senior Agency Official for Privacy (SAOP), and SF apps encrypts all data in transit, uses two factor authentications, time out functions, and event logging in accordance with VA6500 Rev 4.

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?

Only authorized and approved users are given access to PII fields. Data sensitivity is determined by supervisors and the established VBA relationship rules are applied to transactions in these systems.

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

Procedures and controls are documented and submitted to VA OIT's Digital Transformation Center (DTC) following the policies they have in place.

2.4c Does access require manager approval?

Yes. Access requires manager's approval.

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

Supervisors have access to track field updates and not necessarily just PII fields.

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

System owners and supervisors

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

SSN
Name
File Number

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.*

Follows Salesforce VA Org policy for data retention. 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 that are needed for audit purposes 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 National Archives and Records Administration (NARA) General Records Schedules GRS 3.2, item 30 and GRS 3.2, item 31. Records are maintained and disposed of in accordance with the records from this system, 7 years. National Archives and Records Administration (NARA) guidelines as stated in RCS 10-1 records retention schedule requires retention for 75 years. The data retention period has been approved by NARA and is processed according to the following:
General Records Schedule: General Records Schedules (GRS) | National Archives or
https://www.archives.gov/records-mgmt/grs.html

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

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

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

Yes

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

OFM – SF apps follows the VA retention period has been approved by NARA and is processed according to the following:

• General Records Schedule: General Records Schedules (GRS) | National Archives or
https://www.archives.gov/records-mgmt/grs.html

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 are not destroyed every 7 years and records can be queried from system instantiation.

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.

No production PII is used during Testing / Training. All data for training and testing purposes is fictional.

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: Unauthorized access to system may expose PII data.There is a risk that the information maintained 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: Every user needing access is thoroughly reviewed by the supervisor for a suitable level of access to the system inactive users are automatically de-activated by Salesforce after 45days of inactivity The following are true of all VA information system users:
• All employees with access to Veteran's information are required to complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior annually.

• Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.

• Individual users are given access to Veteran's data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user's ID limits the access to only the information required to enable the user to complete their job.

OFM-SF apps do not create, adjust, or make data in any way.

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?

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***
OFM / FMBS/ OFM Applications	Veteran fiscal transactions, date of	File Numbers and Social Security Numbers	Application User Interface internal to module in

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*
	death, beneficiary payments.		Salesforce, no external connection
OFM – BDPR, VBA Finance Center	Veteran fiscal transactions, date of death, beneficiary payments.	FIT Social Security Number, Name, Address, DOB	Application User Interface internal to module in Salesforce, no external connection
OFM Applications SSD Offices OFM Applications	Veteran fiscal transactions, date of death, beneficiary payments.	FIRE Social Security Number, Name	Application User Interface internal to module in Salesforce, no external connection

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: There are a few privacy risks that exists. 1) Unauthorized access: information shared might be accessed by individuals who do not have the authorization, leading to breaches. 2) Data Leakage – potential exposing data to unauthorized third parties who are not authorized to access the data; 3) Misuse of information – information could be misused for purposes other than what it is intended for.

Mitigation: 1) Access to data is managed by supervisors by limiting access to the system 2) Data minimization – users are limited to data as dictated by their data sensitivity levels and relationships. 3) All financial staff are required to complete VA and VBA data protection, data policy and code of conduct training on an annual basis. 4) Auditing of fiscal transactions – activity to transactions are captured in logs and are available to all on the history of the record. 5) Use of secure communication channels – the financial systems are available only when users are

on the VA network in person or thru VPN and encryption is required when sharing sensitive data 6) Implementation of the VA incident response plan for privacy breaches.

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

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.

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

No data is shared with external entities from these applications.

List External Program Office or IT System information is	***List the purpose of information being***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding***	***List the method of transmission and the***

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is no external sharing

Mitigation: There is no external sharing

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.
The system is not collecting any information about the users. SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

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

The system is not collecting information about the users. SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

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.

The system is not collecting any information about the users. SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

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.

The system is not collecting any information about the users. SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

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.
The system is not collecting any information about the users. SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

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: Addressed in SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

Mitigation: Addressed in SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

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.***

The system does not collect information about users. SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.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)?
The system does not collect information about users. SORN for this system is 168VA005, Health InformationExchange-VA 2021-01516.pdf (govinfo.gov)

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?
The system does not collect information about users. SORN for this system is 168VA005, Health InformationExchange-VA 2021-01516.pdf (govinfo.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.

The system does not collect information about users. SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.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.

The system does not collect information about users. SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

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.

The system does not collect information about users. SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

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: The system does not collect information about users. SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

Mitigation: The system does not collect information about users. SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

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?

Individual's Supervisor submits access request to VA OIT's DTC team.
DTC reviews user setup guidelines submitted by OFM.

DTC sends out approval request to system owner to approve user access
System owner, upon thorough review approves/declines the user request

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?

No other agency users have access to this system.

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

Users with access to update Case resolution
Users with access to only view the case
Users with access to just view their own case

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 Contractors do not have access to this system.

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.

All Talent Management System mandated courses for VA Privacy and Security have to be completed prior to gaining access to the system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Not Yet Approved
2. *The System Security Plan Status Date:* N/A
3. *The Authorization Status:* APPROVED
4. *The Authorization Date:* 06/26/2023

5. *The Authorization Termination Date:* 06/26/2026
6. *The Risk Review Completion Date:* 06/23/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate
8.

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

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

Section 9 – Technology Usage

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

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

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

OFM -SF apps are in the cloud model "Software as a Service (SaaS)", and CSP as "Salesforce Government Cloud Plus (SFGCP) Org-VA which is FedRamp approved.

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.*

Yes. Contract entitled: "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B9F0460.

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.

CSP do not collect any ancillary data.

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.

This system is part of Salesforce VA Org which is governed by DTC OIT. DTC OIT ensures CSP (Salesforce) is managing risks within the framework that proactively identifies potential issues with data privacy. Application architecture design is developed based on those guidelines to eliminate issues with privacy of data.

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).

There is one automation that uses bots to create tracer requests in eMPWR-VA and updates status of the Post Payment Workshop (PPW) work item from "Pending Tracer" to "Traced" if the bot is able to create the tracer request. If it is not, the bot updates the PPW work item from "Pending Tracer" to "Pending VBAFC Creation of Tracer" for a human to create the enter the tracer request.

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 provided in this Privacy Impact Assessment is true and accurate.

JASON ANDERSON

Digitally signed by JASON ANDERSON
Date: 2024.10.02 09:57:00 -04'00'

Privacy Officer, Jason Anderson

JAMES BORING

Digitally signed by JAMES BORING
Date: 2024.10.04 13:39:15 -04'00'

Information Systems Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2024.10.11 12:19:15 -04'00'

Information Systems Owner, Michael Domanski

APPENDIX A-6.1

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

SORN for this system is 168VA005, Health Information Exchange-VA 2021-01516.pdf (govinfo.gov)

HELPFUL LINKS:

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

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

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

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

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