Privacy Impact Assessment for the VA IT System called:

VA Profile

Veterans Experience Office
Veterans Affairs

Date PIA submitted for review:

20 September 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dominique Banks	Dominique.Banks@va.gov	(202) 632-8602
Information System Security Officer (ISSO)	Leigh Zirbel	Leigh.Zirbel@va.gov	(605) 336-3230 X93910
Information System Owner	Fred Spence	Fred.Spence@va.gov	(512) 608-5331

Abstract

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

VA Profile is an enterprise master data management (MDM) platform that supports the synchronization and maintenance of VA customers' contact information and communication preferences across VA systems and can provide partner systems a 360 degree view of the Veteran Profile by orchestrating calls to other VA Authoritative Data Sources and combining the data into a single response to the calling Partner.

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?*

VA Profile is a major application owned by the Veteran Experience Office (008) and hosted across 3 Availability Zones in the VAEC AWS GovCloud West. It is managed as a unified system, all compliant with the same controls, by the VA Profile Team and envisions a multi-region future implementation to provide additional geographic separation and improved performance. VA Profile is an enterprise Master Data Management (MDM) solution providing the Veteran a seamless customer experience by consolidating silos of data across the three VA administrations: Healthcare, Benefits, and Burials & Memorials. The data stored will be limited to Veteran Contact Information (identity, name, phone, email, address), Communication Preferences, and a limited amount of Military Personnel Data, as well as some indicators used to assist in processing. Additionally, VA Profile will function as the Data Service to provide Common Data (Needed throughout VA) for a

360-degree view of the Veteran including data elements from VA Profile and the other Authoritative Sources:

- Contact Information (Native)
- Communications Permissions (Native)
- Identity (Master Person Index (MPI))
- Demographics (MPI and Native)
- Socio-Economic (Combined),
- Military Service (VA/DoD Identity Repository (VADIR))
- Experience (Customer Experience Data Warehouse (CxDW)/ Customer Relationship Management (CRM))
- Interaction History (CxDW/CRM)
- Health (Enrollment System (ESR)/Administrative Data Repository (ADR)/ Health Data Repository (HDR)
- Benefits (Corporate Database (VBACORP))
- Memorial Benefits Management System (MBMS)

VA Profile initially ingested data already stored in VBA CORP and Administrative Data Repository (ADR). After additional system integrations and incorporating updates, as of September 2021, VA Profile contains Contact Information on 15.6M Veterans. VA Profile has a Database where its Data is stored, a Common Update Framework (CUF) which coordinates information flow and updates withing the system and a number or services and adapters the perform the necessary transformations to input and output information to and from other systems.

In the event of a system breach, the exposure of Veterans' contact data will seriously harm the reputation of the VA. VA Profile will be the authoritative data source for contact information and has and approved ADS Memo, and has a new SORN in internal review that is more specific to the system as it evolves. The SORN does require Approval in order to supersede the SORN we were operating under. The new SORN does include being hosted in the VAEC. VA Profile's legal authority can be found in Title 38, United States Code, Section 501 and Section 7304.

This PIA is updated with the current and near-term plans of the program and would not trigger any changes. Rejection of this PIA could result in Loss of our ATO and potential shutdown of the system, thereby sacrificing the gains accrued from integrating Contact Information across the various VA Pillars.

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: (S) = Stored, (P) = Passed through.

☒ Name (S)
☐ Social Security Number
☒ Date of Birth (P)
☒ Mother's Maiden Name (P)
☒ Personal Mailing Address (S)
☒ Personal Phone Number(s) (S)
☒ Personal Fax Number (S)
☒ Personal Email Address (S)
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual) (P)
☐ Financial Account Information
☒ Health Insurance Beneficiary Numbers (P) Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Current Medications (P)
☐ Previous Medical Records
☒ Race/Ethnicity (P)
☐ Tax Identification Number
☒ Medical Record Number (P)
☒ Other Unique Identifying Information (P) (list below)

- Other Identifying Numbers
  - VAProfileID (S)
  - PID (P)
  - ICN (P)
  - VPID (P)
  - EDIPI (DoD and Cerner configurations) (S) (P)
- Contact Information BIO (PII including) (S)
  - Personal Address (S)
  - Personal Phone Numbers (S)
  - Personal Email Address (S)
- Benefit Award Bio (PHI including) (P)
  - Award Type (P)
  - Entitlement Amount (P)
- Demographics BIO (PII Including) (P)
  - Race (P)
  - Ethnicity (P)
- Disability Rating BIO (PHI Including) (P)
  - Disability Information (P)
- Military Personnel Data BIO (PII Including) (P)
  - Discharge Status (P)
  - Periods of Service (P)
  - POW Status (P)
  - Service Summary Code (S/P)
- Person Attributes BIO (PFI including)
  - Fraud Indicator (P)
  - Fiduciary Indicator (P)

        - Emergency Response Indicators (P)
        - Active Prescription Indicator
- Health Benefit BIO (PFI/PHI/PII Including) (P)
    - Medical Records (P)
        - Clinical Decisions (Nose/Throat Radium, Military Sexual Trauma, Catastrophic Disability) (P)
        - Special Authorities (Agent Orange, Camp Lejeune Exposure, Radiation Exposure, Shipboard Hazard) (P)
    - Insurance Plans (P)
        - Veteran Health Benefit Plans (P)
        - Healthcare Coverage (P)
    - Associated Persons BIO (P)
        - Next of Kin (P)
    - Benefit Award BIO (P)
    - Demographics BIO (P)
        - Marital Status (P)
        - Religion (P)
    - Disability Rating BIO (P)
    - Person Attributes BIO (P)

PII Mapping of Components

VA Profile consists of 1 key component (database) and access 5 external key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA Profile and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

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**
v36p1a-prd:PRD - VA Profile (VAPRO) - #2203	**Yes**	Yes	Contact Info(Emails, Addresses, Phones) Military Personnel Data (Service Summary Code (SSC)) Person Attributes (Fiduciary, Fraud Indicators)	Storage of PII to enable partner systems to utilize authoritative contact data source.	VA Profile uses FIPS validated encryption in the transfer and storage of PII.

VBACORP (VBA1) – Corporate Database (CRP) - #1153	**Yes**	Yes	Contact Info(Emails, Addresses, Phones) Person Attributes (Fiduciary, Fraud Indicators)	The VBA Corporate Infrastructure provides centralized data storage for many VBA applications, including IRS Tax information and Benefits payment information.	CRP has ATO's in place that establishes their safeguards. Benefits Application Infrastructure - 1373 VBA Corporate Infrastructure - 129
VDRP: VA/DoD Identity Repository (VADIR) - #1682	**Yes**	Yes	Contact Info(Emails, Addresses, Phones) Military Personnel Data (Service Summary Code (SSC))	The Department of Defense is the owner of all data within VDR. The VDR is simply storing this information provided by the DoD and using it to provide an electronic consolidated view of comprehensive eligibility and benefits utilization data from across VA and DoD. VDR stores information on approximately 13 million Veterans.	VADIR has an ATO in place that establishes their safeguards. VA DoD Identity Repository - 126
CDWWork - Corporate Data Warehouse (CDW) - #1152	**Yes**	Yes	Contact Info(Emails, Addresses, Phones) Military Personnel Data (Service Summary Code (SSC)) Person Attributes (Fiduciary, Fraud Indicators)	The Corporate Data Warehouse (CDW)is a business-driven information repository used by key business stakeholders for strategic decision making. The information in the data warehouse is integrated, consistent, detailed, and historical,	CDW has ATO's in place that establishes their safeguards. CDCO-AITC-VHA-CDW Assessing - 139 CDW in Azure - 944

				containing data elements beginning at FY 2000. The CDW contains data from all VistA instances including, but not limited to; clinical, financial, administrative, research, public health, education, policy, performance and quality, patient safety, emergency management, geospatial and surveillance.	
vac20dlsvdweastprod01 - Customer Experience Data Warehouse (CxDW) - #2266	**Yes**	**Yes**	Contact Info(Emails, Addresses, Phones) Military Personnel Data (Service Summary Code (SSC)) Person Attributes (Fiduciary, Fraud Indicators)	Customer Experience Data Warehouse (CxDW) provides a single source of Veteran experience data by collecting information from all Telephone Carriers, Interactive Voice Response (IVR), Automatic Call Distributors (ACD), Customer Relationship Management (CRM), White House Hotline and Survey data across the VA.	CxDW has an ATO in place that establishes their safeguards. Summit Data Platform - 1301
Health Data Repository (HDR II) - #1311	**Yes**	**Yes**	PHI – Active Prescription Records, used to determine if Contact Information updates can be made without	The Health Data Repository II (HDR II) is a data repository of clinical information that resides on one or more independent	HDR II has an ATO in place that establishes their safeguards. Health Data Repository - 113

			impacting critical medication delivery.	platforms and is used by clinicians and other personnel to facilitate longitudinal patient-centric care. HDR II is a relational database that replaces HDR IMS and stores discrete data rather than messages. It enables providers to obtain integrated data views and acquire the patient-specific clinical information needed to support treatment decisions. HDR II serves as the primary source of clinical data for the legal medical record. It maintains data supporting core business functions and serves as a platform for new and re-engineered HealtheVet	

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.

VA Profile is a consolidated location for Veteran contact data. All information stored in VA Profile is sent to VA Profile by VA Partner systems listed below. Other systems update the information because they have direct contact with the veteran and are performing the updates at their request. In the case of VA.Gov the veteran is making the actual change. Other data Identified as "Pass Through" in Section 1.1 above) is provided as a service only and not stored in VA Profile. VA Profile aggregates this data, along with the Contact Information we provide to allow the other system to obtain that 360 degree profile of the Veteran.
Systems providing contact data to VA Profile are:

- Veteran Beneficiary Administration (VBA) Corporate Database (CorpDB), Including their peripheral applications like SHARE, FAS, VETSNET VBMS, EBEN, WINRS and others that change address in CorpDB through BGS
- Veterans Health Administration (VHA) Enrollment System (ESR)/Administrative Data Repository (ADR) including their peripheral applications such as Vista that change addresses in ESR
- Master Person Index (MPI)
- VA.GOV
- VA/DoD Identity Repository (VADIR)
- Cerner Millennium (CM) (Cerner) including their applications JEHR and HIE
- VAEC Mobile Application Platform (VAEC MAP) including their applications Mobile Health Checkup (MAPMHCHECKUP), Virtual Case Manager (MAPVCM)
- VEText (Text Message Appointment Reminders) (VEText) and VA Notify (Telephone Permissions)
- Customer Relationship Management Systems (CRM) SalesForce Based (through Digital Veteran Platform (DVP) Gateway)
    - Caregiver Record Management Application (CARMA)
    - Debt Management Center (DMC)
    - VA Health Connect (Formerly CCCM) Oct 2021
    - Life Insurance Policy Administration Solution (LIPAS)
    - White House Hotline (WHHL) Oct 2021
- Customer Relationship Management Systems Microsoft Dynamics Based (through VEIS Gateway)
    - Member Services (MS-CRM)

VA Profile provides a service consisting of ratings and award data drawn from the Authoritative Data Source.
System providing ratings and awards data:

- VBA Corporate Database (CorpDB)

VA Profile provides a service consisting of health benefits data, drawn from the Authoritative Data Sources.
Systems providing health benefits data:

- Enrollment System (ES)/Administrative Data Repository (ADR)
- Cerner Millennium (CM)

- Health Data Repository (Active Prescriptions)

VA Profile provides a service consisting of Military Personnel/Service data, drawn from the Authoritative Data Sources.
Systems providing health benefits data:

- VA/DoD Identity Repository (VADIR)

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.

VA Profile collects data from the above list of systems by electronic transfer. VA Profile will periodically pull data from partner systems by custom API's or thru data synchronization technologies.
While VA Profile pushes and receives information to and from VBA Corporate database, Administrative Data Repository, Member Services Customer Relationship Management Systems, and Master Person Index, direct updates from the Veteran will occur through va.gov.

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.

VA Profile runs a series of rules to validate contact information received from ADR, VBA Corporate Database, and va.gov in addition to Data corrections sent by the Business Stewards via the VA Profile Business Steward Module (BSM).
Rules include data type validations that ensure incoming messages comply with the required schema, as well as business rules that define the quality standards required to persist information in the authoritative repository. For example, addresses used for correspondence must be deemed deliverable by a Coding Accuracy Support System (CASS) certified vendor.

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

https://www.oprm.va.gov/privacy/systems_of_records.aspx and SORN, please reference 85 FR 52415 SORN #172VA10A7.
Initially under (https://www.govinfo.gov/content/pkg/FR-2020-08-25/pdf/2020-18653.pdf.)
172VA10A7 / 85 FR 52415: The records in this system relate to individuals receiving or providing care at VA or DoD facilities and include health records, identifying information such as Social Security Number, health insurance information, benefits and employee data such as compensation.
A new SORN is being prepared VA Profile Customer Record SORN 192VA30 – In review, not yet filed.

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.

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: VA Profile operates using Personal Identifiable Information (PII). If this information were breached or accidentally released to inappropriate parties or the public, it could result in personal and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: VA Profile will provide a single authoritative and accurate source of Veteran information propagated across the enterprise. The information being collected, used, stored, and disseminated is directly related to providing a single, authoritative source of Veteran contact information. VA Profile does not interact directly with Veterans. VA Profile data is collected thru VA partner applications described in section 1.2 above. VA Profile protects the data by:

1) Minimizing access - Less than 50 total Business Data Stewards have access to the contact data repository thru the Business Steward Module (BSM) – BSM is being discontinued.

2) Interactions through partner systems are secured by those partners and covered under their PIA's and ATO's. As BSM is discontinued, VA Profile Data Quality team will review and monitor the data quality and alert any partner systems where data quality issues are observed so that corrective actions may be determined and acted upon.

3) Restricting access - VA Profile Business Stewards and Data Quality team members must be on the Veteran Affairs network and must use two-factor authentication using a Veteran Affairs issued Personal Identity Verification (PIV) card.

4) Data Encryption - VA Profile encrypts data in transit and data stored in the VA Profile database using FIPS 140-2 compliant encryption. VA Profile employ a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures 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. VAEC AWS GovCloud employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

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 following data types are used by Business Steward Module (BSM) Data Stewards to validate the identity of the individual prior to making changes to the contact record.

- Name

- Date of Birth
- Mother's Maiden Name

VA Profile is the authoritative data source for contact information at the VA. The following fields are used to synchronize the information with approved systems for contacting the Veteran.

- Addresses
- Zip Code
- Phone Numbers
- Fax Number
- Email Address

The following data is provided by VA Profile as a service from other systems for the purposes of completing key business processes within VHA and VBA.

- Benefit Award Bio (PHI including) (P)
    - Award Type (P)
    - Entitlement Amount (P)
- Demographics BIO (PII Including) (P)
    - Race (P)
    - Ethnicity (P)
- Disability Rating BIO (PHI Including) (P)
    - Disability Information (P)
- Military Personnel Data BIO (PII Including) (P)
    - Discharge Status (P)
    - Periods of Service (P)
    - POW Status (P)
    - Service Summary Code (S/P)
- Person Attributes BIO (PFI including)
    - Fraud Indicator (P)
    - Fiduciary Indicator (P)
    - Emergency Response Indicators (P)
    - Active Prescription Indicator
- Health Benefit BIO (PFI/PHI/PII Including) (P)
    - Medical Records (P)
        - Clinical Decisions (Nose/Throat Radium, Military Sexual Trauma, Catastrophic Disability) (P)
        - Special Authorities (Agent Orange, Camp Lejeune Exposure, Radiation Exposure, Shipboard Hazard) (P)
    - Insurance Plans (P)
        - Veteran Health Benefit Plans (P)
        - Healthcare Coverage (P)
    - Associated Persons BIO (P)
        - Next of Kin (P)
    - Benefit Award BIO (P)
    - Demographics BIO (P)
        - Marital Status (P)
        - Religion (P)
    - Disability Rating BIO (P)

- Person Attributes BIO (P)

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

VA Profile does not create new data. It validates contact data and acts as a master contact data source.

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?

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

Add answer here:

VA Profile use FIPS validated encryption in the transfer and storage of PII. Social Security Numbers are not processed or stored in VA Profile. Master Person Index (MPI) may transmit SSN's in some of their packets, but VA Profile drops those portions of data and does not store or process.

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

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:

Access to the VA Profile contact data is highly restricted to only authorized Veteran Affairs systems and VA Profile Business Stewards. VA Profile Access Control (AC) Standard Operating Procedure defines the roles and procedures for gaining access. VA Systems exchanging data with VA Profile utilize certificate-based authentication and communication partners are limited by network access control lists (ACL).
All VA Profile Business Stewards must request access to the VA Profile Business Steward Module (BSM) and all requests must be approved by the appointed by the VA Profile Business Lead. All access is monitored, tracked, recorded and periodically reviewed in compliance with VA requirements and NIST guidelines.

Section 3. Retention of Information

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

3.1 What information is retained?

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

Name, Date of birth, Mother's Maiden Name, Mailing Address, Zip Code, Phone Numbers, Email 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 Profile records are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. The records are disposed of in accordance with General Records Schedule 20, item 4. Item 4 provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes.

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 Profile retention of identified data types have been approved by The VA records office and the NARA for the prior SORN as modified by is latest revision. The VA Profile new SORN submission matches this schedule.

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

If Sensitive personal information, such as name needs to be eliminated from the system, the approved processes present at that time will be followed. Since this could occur up to 80 years from this time, it is difficult to forecast those processes. When data is transferred to a separate facility, sensitive IT electronic storage and memory devices are used, and proper clearing procedures are required to remove any residual data.
In accordance with VA Directive 6371 Destruction of Temporary Records, it is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, and the GRS Schedule 20, item 4. GRS can be found at www.archives.gov. VA Directive 6300, Records and Information Management contains the policies and responsibilities for VA's Records and Information Management program. VA Handbook 6300.1, "Records Management Procedures", Section 3.2, contains mandatory procedures for the proper management of eliminating data at the end of the retention period. Procedures are enforced by Records Management Staff and VA Records Officers.
Additionally, VA Profile will comply with VA Directive 6500, NIST SP 800-53, Control DM-2 as documented in EMASS

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

VA Profile may use PII data for testing the application in a secured Pre-Production environment. VA Profile's Pre-Production environment is equal to the Production environment and is included in the authorization boundary. PII data is not used for research or testing in any other environments below Pre-Production or Production.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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:
<u>Privacy Risk:</u> There is a risk that the information maintained by VA Profile 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.

<u>Mitigation:</u> To mitigate the risk posed by information retention, VA Profile adheres to the disposition authority approved by the Veteran Affairs and the Archivist of the United States., Sensitive personal information, such as name, are never eliminated from the system. When data is transferred to a separate facility, sensitive IT electronic storage and memory devices are used and proper clearing procedures are required to remove any residual data.

In accordance with VA Directive 6371 Destruction of Temporary Records, it is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, and the GRS Schedule 20, item 4. GRS can be found at www.archives.gov. VA Directive 6300, Records and Information Management contains the policies and responsibilities for VA's Records and Information Management program. VA Handbook 6300.1, "Records Management Procedures", Section 3.2, contains mandatory procedures for the proper management of eliminating data at the end of the retention period. Procedures are enforced by Records Management Staff and VA Records Officers.
Additionally, VA Profile will comply with VA Directive 6500 Control DM-2
· VA will retain PII for the minimum amount of time to fulfill the purpose(s) identified in the notice or as required by law;
· Dispose of, destroy, erase, and/or anonymize the PII regardless of the method of storage in accordance with a NARA-approved record retention schedule and in a manner, that prevents loss, theft, misuse, or unauthorized access; and
· Use approved records disposition schedules to ensure secure deletion or destruction of PII (including originals, copies, and archived records).
· Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods

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 3.10 (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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Experience Office	(IAM MPI) IAM – Master Person Index (IAM MPI) #1406	Contact Information BIO Person Attributes Bio Personal Traits Person Identity (identity correlations, mother's maiden name, gender, DOB, SSNLast4, patient, date of death) *(SSN is transmitted from MPI to VAPROFILE in the identity correlation lookup (HL7 1305/1306 messages). VA Profile does not collect, process, retain or share this data.)*	SOAP (Simple Object Access Protocol) Web Service Using HTTPS (Hypertext Transfer Protocol Secure) with MTLS (Mutual Transport Layer Security)
Veterans Benefits Administration	Corporate Database #1153	Contact Information BIO Award Events	Oracle GoldenGate Using TCPS (Transfer Control Protocol with SSL), JDBC (Java Database Connectivity) Using TCPS (Transfer Control Protocol with SSL) to VBA Corporate Repository, SOAP (Simple Object Access Protocol) Web Service Using HTTPS (Hypertext Transfer Protocol Secure) (one-way)

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 shared/received with the Program Office or IT system*	*Describe the method of transmittal*
Veterans Benefits Administration	(VBMS) Veterans Benefits Management System #1728	Contact Information BIO	RESTful (Representational state transfer) Web Service Using HTTPS (Hypertext Transfer Protocol Secure) with MTLS (Mutual Transport Layer Security)
Veterans Benefits Administration	Veterans Experience Integration Solution (VEIS) - #2405 – (Gateway) Accessing through this Gateway: Member Services - Customer Relationship Management (MS CRM) - #2056	Contact Information BIO Person Attributes Bio	REST (PUT and POST) over HTTPS using MTLS
Veterans Benefits Administration	Electronic Virtual Assistant (e-VA) - #2419	Contact Information BIO	REST (Representational state transfer) (GET,PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security)
Veterans Benefits Administration	Veteran Readiness and Employment Case Management System (VRE-CMS) #2058	Contact Information BIO	REST (Representational state transfer) (GET,PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security)
Veterans Benefits Administration	Benefit Gateway Services (BGS) #5073	Fraud Fiduciary Ratings Awards	SOAP (Simple Object Access Protocol) Web Service Using HTTPS (Hypertext Transfer Protocol Secure) with MTLS (Mutual Transport Layer Security)
Veterans Benefits Administration	Life Insurance Policy Administration Solution (LIPAS) #2404	Contact Information BIO	REST (Representational state transfer) (GET,PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security)

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 shared/received with the Program Office or IT system*	*Describe the method of transmittal*
Veterans Health Administration	(ESR) Enrollment System Redesign (ESR) #1231 Includes Veteran Information Systems Technology Architecture (VistA) #1973	Contact Information BIO Health Benefit BIO (associations,Health Care coverages, disability rating, demographics, clinical decision, medals and awards) Demographics BIO Disability Rating BIO Benefit Award Bio	RESTful (Representational state transfer) Web Service Using HTTPS with MTLS (Mutual Transport Layer Security)
Veterans Health Administration	Caregiver Record Management Application (CARMA) - #2475	Contact Information BIO	REST (Representational state transfer) (GET,PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security)
Veterans Health Administration	Health Data Repository (HDR) #1311	Prescription Information	SOAP (Simple Object Access Protocol) Web Service Using HTTPS (Hypertext Transfer Protocol Secure) with MTLS (Mutual Transport Layer Security)
Veterans Experience Office	Veteran Facing Services Platform - va.gov (formerly Vets.gov Website) (Vets.gov) #2103 (VA.gov) #1681	Contact Information BIO Communications Permission BIO Communications Permission Configuration BIO	RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security)
Veterans Experience Office	(VADIR) VA/DoD Identity Repository (VADIR) #1682	Contact Information BIO	Oracle GoldenGate Using TCPS (Transfer Control Protocol with SSL)

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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Office of Information Technology	VAEC Mobile Application Platform (VAEC MAP) - #2313 (Includes the following Apps through MAP) MAPMHCHECKUP MAPSOMNOWARE MAPVCM	Contact Information BIO	REST (Representational state transfer) (GET,PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security)
Office of Information Technology	Digital Veterans Platform (DVP) #2196	Contact Information BIO Person Attributes Bio	REST (Representational state transfer) (GET,PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security)
Office of the Chief Technology Officer	VEText (Text Message Appointment Reminders) (VEText) - #2253 Includes VA Notify	Contact Information BIO Communications Permission BIO Communications Permission Configuration BIO	REST (Representational state transfer) (GET,PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security)
Financial Services Center	Electronic Document Management - Debt Management Center (EDM-DMC) - #2229	Contact Information BIO	REST (Representational state transfer) (GET,PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security)

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 PII is that sharing data within the Department of Veteran's Affairs could happen and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by the VA Profile Business Stewards. Only personnel with a clear business purpose are allowed access to the system and the information contained within, as identified in Section 2.4 above.

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 3.11 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 shared/received 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*
Cerner Millennium (CM) - #2204		Contact Information BIO Health Benefit	National MOU/MOA	REST (Representational state transfer)

Office of the Principal Deputy Under Secretary for Health Product Line: Electronic Health Record Modernization		BIO Demographics BIO Disability Rating BIO Benefit Award Bio		(PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security)
Joint Health Information Exchange (JHIE) #11239 (Cerner Component) Department of Defense: Defense Health Agency		Contact Information BIO Health Benefit BIO Demographics BIO Disability Rating BIO Benefit Award Bio	National MOU/MOA	REST (Representational state transfer) (PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security)

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:
Privacy Risk: The privacy risk associated with sharing PII data with Cerner and DoD is that the data may be disclosed to individuals who do not require access and this heightens the threat of the information being misused.

Mitigation: The DoD and Cerner systems have ATO's and those systems' management of sensitive and PII data is well defined in their respective security plans and privacy impact assessments. The network interface between VA Profile and the external systems route through the VA's Trusted Internet Connections (TIC) and are fully compatible with VA, DoD, and Federal security policies and protocols.

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.

VA Profile receives its data collection from VA Partner Systems. VA Partner Systems provide adequate notification by giving public notice of data collection via the Federal Register. Additional notices and terms of use are posted on web pages and physical forms that the individual directly interacts with.
Notice is provided to individuals prior to data collection and data exchange with VA Profile. A System of Records Notification (SORN) was published in the Federal Register on August 25, 2020. Please reference 85 FR 52415 and SORN #172VA10A7.

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

VA Profile does not provide an opportunity to decline to provide information. Data stored by VA Profile is received from VA application partners. VA Profile does not collect any information directly from Veterans or their dependents.

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

VA Profile does not provide a consent option of data use to the Veteran. Data stored by VA Profile is received from VA application partners. VA Profile does not collect any information directly from Veterans or their dependents.

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 individuals who provide information to the VA Profile application partners will not know how their information is being shared and used internal to the Department of Veterans Affairs.

Mitigation: SORN # 172VA-10A& and publication of 85 FR 52415 provides notice to the individual of how the data collected will be utilized within the Veteran Affairs

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.

In accordance to VA Directive 6300 and Handbooks 6300.3, Procedures for Implementing the FOIA, 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act, and VHA Directive 1605.1, Privacy and Release of Information an individual's submitting information requests may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned system of records, Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted

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

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

Individuals are able to correct inaccurate or erroneous information by contacting the VA partner system (such as VA.gov) in which they are registered. Individuals will follow procedures for correcting individuals' information maintained by the Veteran Beneficiary Administration (VBA) Corporate database and the Master Veterans Index (MVI)

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

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

Individuals are made aware of correcting his or her information from the VA Partner system that interacts with VA Profile. Veteran Beneficiary Administration (VBA) Corporate database and the Master Person Index are responsible for providing notice and directions to individuals on how to correct their individual information.

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.

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

If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before with the VA Partner system, and state that the documentation they are now providing supersedes that previously provided.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:
<u>Privacy Risk:</u> There is a risk that the information provided to VA Profile is inaccurate and decisions are made with incorrect information

<u>Mitigation:</u> VA Profile and VA Partner Systems follow VA processes which allow an individual, adequate notification of the data being collected and the limitations of use for the data as indicated in the SORN. The Master Veterans Index and CORP database provide procedures that allow individuals to correct inaccurate data

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.

VA Profile functions as a back-end system and provides a single web interface for VA Data Stewards. All access to its services and interfaces is within the VA internal network. VA partner applications interact directly with the VA Profile through authenticated application calls or thru data synchronizations services.
VA Profile Access Control (AC) Standard Operating Procedure defines the roles and procedures for gaining access.

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.

Contractors will have access to the VA Profile system and contact data containing PII. All contractors must be cleared, approved, complete required Security and Privacy training and accept the VA Rules of Behavior prior to access being granted. Two functional contract teams provide services for VA Profile.
The VA Profile application development and sustainment team have access to the VA Profile database and applications. They are responsible for the overall design and functionality of the VA Profile application. The Prime Contractor Signs the BAA and NDA with VA, and ensures each subcontractor signs the BAA at the company level and each direct employee and subcontractor employee signs the non-disclosure agreement. These documents are maintained by the Prime Contractor.
VA Profile contracts are reviewed at least annually by the VA Contract Officer Representative (COR) Per VA Handbook 6500.6 requirements.

VA Profile Access Control (AC) Standard Operating Procedure defines the roles and procedures for gaining 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 security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session. Annual training records and acceptance of the Rules of behavior are maintained in the VA Talent Management System (TMS):

- Privacy and HIPPA Training
- VA Privacy and Information Security Awareness and Rules of Behavior

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

If Yes, provide: As documented in VASI #2203 and EMASS VA Profile - 207

1. The Security Plan Status,	**APPROVED**
2. The Security Plan Status Date,	**03-Dec-2020**
3. The Authorization Status,	**Authorized to Operate (ATO)**
4. The Authorization Date,	**07-Jan-2021**
5. The Authorization Termination Date, .	**07-Jan-2022**
6. The Risk Review Completion Date	**21-Dec-2020**
7. The FIPS 199 classification of the system	**HIGH**

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.***

N/A

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, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

VA Profile is hosted in the VAEC and further information can be found in the VAEC PIA.

9.2 Identify the cloud model being utilized.

Example: 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.

VA Profile is hosted in the VAEC and further information can be found in the VAEC PIA.

9.3 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.

VA Profile is hosted in the VAEC and further information can be found in the VAEC PIA.

9.4 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.

VA Profile is hosted in the VAEC and further information can be found in the VAEC PIA.

9.5 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.

VA Profile is hosted in the VAEC and further information can be found in the VAEC PIA.

9.6 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 employ Robotics Process Automation.

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 provided in this Privacy Impact Assessment is true and accurate.

Dominique A. Banks 747748

Digitally signed by Dominique A. Banks 747748
Date: 2021.09.30 11:21:58 -04'00'

Privacy Officer, Dominique Banks

LEIGH A. ZIRBEL 252119

Digitally signed by LEIGH A. ZIRBEL 252119
Date: 2021.09.30 13:13:58 -05'00'

Information Systems Security Officer, Leigh Zirbel

Fred V. Spence 750842

Digitally signed by Fred V. Spence 750842
Date: 2021.09.30 13:27:30 -05'00'

System Owner, Fred Spence

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).

https://www.govinfo.gov/content/pkg/FR-2020-08-25/pdf/2020-18653.pdf