Privacy Impact Assessment for the VA IT System called:

# VA Profile

# VA Central Office (VACO)

# Veterans Experience Office (VEO-30)

# eMASS ID # 207

Date PIA submitted for review:

17 Dec 2024

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Anmar Faik | anmar.faik@va.gov | 202-459-8385 |
| Information System Security Officer (ISSO) | Clyde “Butch” Johnson | Clyde.Johnson1@va.gov | 423-979-1407 |
| 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 for VA?".*

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 Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

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 purpose of VA Profile is to serve as the authoritative data source for common customer profiles of Veterans; their families, caregivers, and survivors; and other VA customers. The profile data in this system of records is mastered and synchronized with information in other data sources, meet VA data quality standards, and is updated using a single touchpoint service. Through synchronization of information from various data sources, VA Profile provides VA administrations and program offices with a customer profile that is accurate, relevant, complete, and timely.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

VA Profile (eMASS #207) is a major application which is VA Owned, VA Operated, 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.

*2. Information Collection and Sharing*

C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

VA Profile is the Authoritative Data Source for Contact Information, and is requesting that designation for Demographics (Race, Religion, Ethnicity, Marital Status, and

Preferred Language), and Communication Permissions for Veterans, Beneficiaries and Caregivers. Currently there are over 34.5 million individuals with some of this data stored in VA Profile. This data is shared directly with VA Systems, Oracle Health and other Partners with VA ATO's. Some of these partners may share some of this data with other systems as documented in those systems ISA/MOU/CMA's. VA Profile is system to system only connections and does not support an end user Interface. Records in the system contain information about Veterans; their families, caregivers, and survivors; and eligible beneficiaries who are receiving or have received title 38 benefits and services; and other individuals who may be entitled to title 38 benefits and services.

| **Check if Applicable** | **Demographic of individuals** |
|---|---|
| ☒ | Veterans or Dependents |
| ☐ | VA Employees |
| ☐ | Clinical Trainees |
| ☐ | VA Contractors |
| ☐ | Members of the Public/Individuals |
| ☐ | Volunteers |

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

VA Profile modernizes VA systems by ensuring that VA customer common data is synchronized and shared across the VA, regardless of the channel used to update the information. Synchronizing data across major VBA, VHA and NCA systems is just one step in synchronizing all VA systems. Over time, VA Profile will be adding new VA systems and business lines so Veterans' identity, contact information, military service, enrollment, eligibility for VA services and benefits, socio-economic, demographic, customer experience, interaction history and shared data from health, benefits and cemetery administrations are automatically synchronized across all VA systems. VA Profile will become the authoritative data source for VA common data. VA Profile will provide VA customers the ability to update information and have a 360° view of their Master Record and improve data quality and management of the Veteran profile through implementation of business rules and exception handling within the solution, as well as enterprise data governance (policy, procedures, etc.). The customer record will be readily available for the Veteran and VA staff to view through integrated partner's interfaces. VA Profile employs an enterprise Master Data Management

(MDM) solution. The MDM provides a capability for VA master data that supplies a cleansed, singular, authoritative set of information comprising all applicable data subject areas shared among multiple Lines of Business (LoBs). MDM data updates will be propagated to relevant consuming systems in all applicable LoBs; VA customers will be enabled to update contact, demographic and socio-economic information for immediate propagation VA-wide to avoid the need for duplicate data entry. The VA Profile Longitudinal Veteran Record VA Profile solution will result in creation of an Enterprise Services domain system which creates the nucleus for the Enterprise Data Management (EDM) solution.

E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

The objective of a Master Data Management system is to share accurate, authoritative data with other systems. VA Profile supports partners enabling them to retrieve the 360-degree view of the veteran information, based on their business needs (only data needed is approved), through VA Profile from the Authoritative Data Sources.

VA Profile has implemented a Security Service that controls access for each partner to the services and data Business Interface Objects (BIO) that are shared with the partner. The picture below shows a sample partner permission.

### *Role Based Partner Permissions*

| Partner | App Role | User Role | Permissions | User Role Create Date | User Role Update Date |
|---|---|---|---|---|---|
| SAMPLE | contact-information-hub | mdm.cuf.contact.information.service.dio.AddressDio | Read | 7/23/2024 | 9/23/2024 |
| SAMPLE | contact-information-hub | mdm.cuf.contact.information.service.dio.ContactInformationDio | Read | 7/23/2024 | 9/23/2024 |
| SAMPLE | contact-information-hub | mdm.cuf.contact.information.service.dio.EmailDio | Read | 7/23/2024 | 9/23/2024 |
| SAMPLE | contact-information-hub | mdm.cuf.contact.information.service.dio.TelephoneDio | Read | 7/23/2024 | 9/23/2024 |
| SAMPLE | military-personnel | MilitaryPersonnelSummaryBio | Read | 7/23/2024 | 9/23/2024 |
| SAMPLE | military-personnel | MilitaryServiceEpisodeBio | Read | 7/23/2024 | 9/23/2024 |
| SAMPLE | military-personnel | MilitaryServiceHistoryBio | Read | 7/23/2024 | 9/23/2024 |
| SAMPLE | military-personnel | PayGradeRankBio | Read | 7/23/2024 | 9/23/2024 |
| SAMPLE | military-personnel | ServiceAcademyEpisodeBio | Read | 7/23/2024 | 9/23/2024 |
| SAMPLE | military-personnel | ROLE_MILITARY_PERSONNEL | User | 7/23/2024 | 9/23/2024 |
| SAMPLE | military-personnel-corp | ROLE_MILITARY_PERSONNEL_CORP | User | 7/23/2024 | 9/23/2024 |
| SAMPLE | Person-mdm-cuf-person-hub | mdm.cuf.person.server.dio.PersonDio | Read | 7/23/2024 | 9/23/2024 |

The table below maps the PII/PHI to the Services that support these interfaces and the data retrieval and sharing.

*PII Mapped to Services*

| **Service Name - Application Program Interface (API) that contains PII/PHI** | **Specifically list the PII/PHI Data Elements Sharing (Internally)** |
|---|---|
| BOLD TEXT indicates Data stored in VA Profile | |
| ○ Award Service<br>▪ Benefit) Award Bio (PHI) | • Financial Info, Medical History |
| ○ **Contact Info Service**<br>▪ **Contact Information BIO (PII)** | • Personal Address, Phone & Email |
| ○ **Demographics Service**<br>▪ **Demographics BIO (PII)** | • Race, Ethnicity |
| ○ Gender Identity Traits<br>▪ Gender Identity Traits (PII) | • Gender |
| ○ **Airborne Hazards Burnpit (PHI)**<br>▪ **AHOBPR Indicator** | • Military History |
| ○ **Customer Interactions Service**<br>▪ **Customer Interaction History (PII/PHI)** | • Veteran Interactions |
| ○ Health Service<br>▪ Health Benefit BIO (PFI/PHI/PII) | • Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers |
| ○ Military Personnel Data<br>▪ Military Person (PII) | • Military History |
| ○ Person<br>▪ Person Attributes BIO (PFI/PHI) | • Financial, Medications, Medical Records |
| ○ Disability Ratings Service<br>▪ Ratings Data (PF/PHII) | • Service Connection/Disability |
| ○ Profile Service<br>▪ **All above except Customer Interaction** | |

F. *Are the modules/subsystems only applicable if information is shared?*

Partners access is granted by application role and user role. If the partner has not been granted permissions on a specific data domain, or BIO, then they will not receive any data for that domain/BIO, they will instead receive and error that they do not have permissions and a log entry will be created indicating which partner was attempting to access what data area without permission.

*G. Is the system operated in more than one site to include primary and secondary 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?*

VA Profile is 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. Provisioning the second region has started.

*3. Legal Authority and System of Record Notices (SORN)*

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

https://www.govinfo.gov/content/pkg/FR-2023-10-23/pdf/2023-23327.pdf and SORN, please reference 88 FR 72820.

*H. What is the SORN?*

https://department.va.gov/privacy/system-of-records-notices/, please reference SORN 192VA30.

*I. SORN revisions/modification*

This is the latest modified version.

*I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

Modification already completed.

*4. System Changes*

*J. Will the business processes change due to the information collection and sharing?*

*☐ Yes*<br>
*☒ No*<br>
*if yes, <<ADD ANSWER HERE>>*

*K. Will the technology changes impact information collection and sharing?*

*☐ Yes*<br>
*☒ No*<br>
*if yes, <<ADD ANSWER HERE>>*

## 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 Information 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/](https://vaww.va.gov/vapubs/)). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.*

*If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.*
*This question is related to privacy control AP-1, Authority to Collect, and AP-2, Purpose Specification.*

*The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.*

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
☒ **Full** Social Security Number
□ **Partial** 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/Sex
☒ Integrated Control Number (ICN)
☒ Military History/Service Connection
☒ Next of Kin
☒ Date of Death
□ Business Email Address
☒ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (list below)

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

Other PII/PHI data elements: (S) = Stored, (P) = Passed through.

- Other Identifying Numbers
    - VAProfileID (S)
    - PID (P)
    - ICN (P)
    - VPID (P)
    - EDIPI (DoD and Cerner configurations) (S) (P)
    - Other Coorelated ID's stored in MPI (P)
- Contact Information BIO (PII including) (S)
    - Personal Residential Address (S)
- Benefit Award Bio (PHI including) (P)
    - Award Type (P)
    - Entitlement Amount (P)
- Demographics BIO (PII Including) (S)
    - Marital Status (S)
    - Religion (S)
- Gender Identity Traits (P)
    - Preferred name (P)
    - Pronoun (P)
    - Gender Identity (P)
    - Sexual Orientation (P)
- Airborne Hazards Burnpit (S)
- Customer Interaction History (S)
    - Veteran Interaction Records (P)
- Disability Rating BIO (PHI Including) (P)
    - Service Connection/Disability (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)

### 1.2 List 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?*

VA Profile is a consolidated location for Veteran Contact Information, Demographics, Interaction History and Airborne Hazards Burnpit indicators. 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
- Integrated Schedule Solution (ISS) is a component related to VHA ESR and is used by VA Staff scheduling appointments for veterans and updating their information during the process.
- Master Person Index (MPI)
- VA.GOV
- VA/DoD Identity Repository (VADIR) – Contact Information Records for Servicemembers are shared with VA Profile and are used to update records, when no VA Collected data is present or recorded.
- 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)
- Digital GI Bill (DGIB)
- 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 (VAHC)
    - 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)

*Systems providing Demographics data to VA Profile are:*

- Veteran Health Administration (VHA) Enrollment System (ESR)/Administrative Data Repository (ADR) including their peripheral applications such as Vista that change addresses in ESR
- Integrated Schedule Solution (ISS) is a component related to VHA ESR and is used by VA Staff scheduling appointments for veterans and updating their information during the process.
- VA/DoD Identity Repository (VADIR) is integrated with DoD and is the source of Military Personnel Data within VA. Demographic Records for Servicemembers are shared with VA Profile and are used to update records, when no VA Collected data is present or recorded.

*System providing Airborne Hazards Burnpit and Interaction History data to VA Profile is:*

- Summit Data Platform

VA Profile provides services 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)

VA Profile provides services for Gender Identity, and correlation records to facilitate cross source information retrieval.

*System providing identity data:*

- VA Master Person Index (VA MPI)

*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.*

VA Profile is a consolidated location for Veteran Contact Information, Demographics, Interaction History and Airborne Hazards Burnpit indicators. All information stored in VA Profile is sent to VA Profile by VA Partner systems listed above. 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. VA Profile provides orchestrated information from VA Systems to partner systems, thus multiple calls to MPI and other systems are reduced and the overall the efficiency of the entire VA is improved.

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

VA Profile does not create information. It does have monitoring and metrics that report on various statistic in the system such as Number of Records, Percentage of data completion, etc.

**1.3 Methods of information collection**

*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?*

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.

*1.3b 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?*

No forms are used to collect information.

**1.4 Information checks for accuracy, and 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.*

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.

*1.4b 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?*

No Commercial aggregator of information is used.

**1.5 Identify the specific legal authorities, arrangements, and agreements that 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*

> 88 FR 72820 - Privacy Act of 1974; System of Records - Content Details - 2023-23327
> Federal Register Volume 88, Issue 203 (October 23, 2023)
> SORN: 192VA30/87 FR 36207,
> Title: Veterans Affairs Profile-VA (VA Profile) (192VA30).

**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: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

*Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.*

*Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.*

*Principle of Data Quality and Integrity:* *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*
*This 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) Interactions through partner systems are secured by those partners and covered under their PIA's and ATO's. The 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.

2) Restricting access - VA Profile 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.

3) 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 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 |
|---|---|---|
| VA Profile ID | Internal Record Identification | Not used |
| EDIPI | Correlated Record Identification | Not used |
| Personal Mailing Address | Communication/Correspondence | Not used |
| Personal Residential Address | Communication/Correspondence | Not used |
| Personal Phone Numbers | Communication/Correspondence | Not used |
| Personal Email | Communication/Correspondence | Not used |
| Race/Ethnicity | Demographics Analysis | Not used |
| Marital Status | Demographics Analysis | Not used |
| Religion | Demographics Analysis | Not used |
| AHOBPR Indicator | Eligibility Indication | Not used |
| Customer Interactions | Communication Reference | Not used |
| Service Summary Code (MPD) | Eligibility Determinations | Not used |
| PID, ICN, Other ID's | Record Correlation and Query | Not used |
| Award Type | Benefits Analysis and Determination | Not used |
| Entitlement Amount | Benefits Analysis and Determination | Not used |
| Preferred Name | Veteran Interactions per their preferences | Not used |
| Pronoun | Veteran Interactions per their preferences | Not used |
| Gender Identity | Veteran Interactions per their preferences | Not used |
| Sexual Orientation | Veteran Interactions per their preferences | Not used |
| Service Connection/Disability | Benefits/Program qualification/determination | Not used |
| Discharge Status | Benefits/Program qualification/determination | Not used |
| Periods of Service | Benefits/Program qualification/determination | Not used |
| POW Status | Benefits/Program qualification/determination | Not used |
| Service Summary Code | Benefits/Program qualification/determination | Not used |
| Fraud Indicator | Record Update Decisions | Not used |
| Fiduciary Indicator | Record Update Decisions | Not used |
| Emergency Response Indicator | Record Update Decisions | Not used |
| Active Prescription Indicator | Record Update Decisions | Not used |
| Medical Records (P)<br>Clinical Decisions<br>(Nose/Throat Radium, Military Sexual Trauma, Catastrophic Disability)<br>Special Authorities<br>(Agent Orange, Camp Lejeune Exposure, Radiation Exposure, Shipboard Hazard) | Eligibility, Treatment | Not used |
| Insurance Plans | Healthcare Coverage | Not used |
| Associated Persons | Healthcare | Not used |

### 2.2 Describe the types of tools 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?*

VA Profile is a real-time system which conducts limited analysis on the data to make the assessments of data quantity, data quality, data completeness and error/transaction volume analysis. No data other than performance metrics are created. Data from VA Profile is shared with CXi which is a is used for Reporting and Analysis of the information.

*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.*

The only new information created about individual records are the addition of the provenance data (source of and data/time of data change/input) and the audit records. Provenance data is available to consuming systems on subsequent data retrieval. Audit records are not generally accessible other than for system/database administrators (those with elevated privileges).

### 2.3 How the information in the system is 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?*

VA Profile use FIPS validated encryption in the transfer and storage of PII.

*2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).*

Social Security Numbers may be received from partners and transmitted to MPI as traits for the purpose of determining identity, in conjunction with other traits. Other than system logs required for audit purposes, Social Security Numbers are not stored within the database.

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

VA Profile is a backend system connecting with other systems. Partners requesting data go through an intake process to have the needs of the consuming system evaluated and ensure that only the data needed is made available once approved. If not approved by the Data

Stewards/Authoritative Data Sources (ADS), access is not granted. When access is approved, the Permissions Granted are only for those Business Interface Objects (BIO's) that were approved in the intake. Any requests for elements not included in the approved list are logged and tracked in anomaly reports, resulting in the Outreach to the Partner to inform them that they are requesting information they are not authorized to have, and as such, the information was not provided. Partners are requested/required to correct the request or substantiate the approved need for that data. All individuals (admins, dba, analysts) internal to VA Profile who need access to all data have Elevated Privileges Requests submitted and approved prior to access grant and are thus bound to follow VA Policies with Annual Training.

**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?*

Partner systems access is requested through the Information Technology Request Portal, by submitting an intake request. This is reviewed by the VEO Business Office (VA Profile Product Owner), VA Profile Data Governance/Quality Team, and the VA Profile Product Manage to approve the partner systems need to access and their ATO status respective to the data being requested. Partner Systems manage the access to data within their boundary. Individual's access to data is restricted to approved development and support personnel. VA PROFILE ensures that all users remain compliant per National Institute of Standards and Technology (NIST) and VA Policies and Regulations. The Standard Operating Procedure (SOP) (referenced in 2.4b below) document specifies procedures allowing standardization and continuity of process for Access Control functions VA PROFILE. This SOP enhances A&A compliance in the (Access Control) (AC) control family, coordinates with control inheritance sources, and reduces procedural variation due to personnel, life cycle, regulatory or VA organizational changes.

VA PROFILE ensures that all users remain compliant per National Institute of Standards and Technology (NIST) and VA Policies and Regulations. This SOP addresses the AC procedures facilitating implementation of Access Control policy and associated requirements. In addition, this

SOP is guidance for review and updating AC control procedures. This SOP directly supports the VA Risk Management Framework (RMF

*2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?*

All criteria, procedures, controls, and responsibilities regarding access is documented in VA Profile_AC_SOP_09162024_EB.pdf, approved and documented in eMASS.

*2.4c Does access require manager approval?*

As documented in the SOP (above), manager approval is required, and must be documented within the approved VA systems and tools.

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

Access is monitored, tracked and recorded in accordance with the SOP above. These are stored in system Logs, Audit tables and other tools for monitoring. Interactions with Partner systems are tracked at the system level, and data changes where VA Profile is the Authoritative Data Source(ADS) are tracked down to the Source System user wherever possible. Individual (Support team) interactions are tracked at the person/transaction level.

*2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?*

The Information System Owner and the Operations and Maintenance team of VA Profile perform these functions as documented in SOP referenced above. Specifically:

- Information System Owner (ISO)
    - Ensure adherence to Access Control Policy by VA staff and contractors.
    - Responsible for approving and signing Access Control policies and procedures.
    - Provide oversight for personnel with significant responsibility to information systems.
    - Update procedures as needed to ensure it meets OIT mission requirements and complies with Federal Laws, Policies, Procedures, and Guidelines.
    - Ensure all procedures herein are properly complied with
- Product/Business Owner; Program/Project Manager; Contracting Officers Representative (PM; COR)
    - Ensures the VA PROFILE development and redaction contractors complies with the AC SOP.
    - Provides approval for group membership to VA PROFILE Development/Contractor.
    - Fulfills role of Account Manager for access to VA PROFILE.
        - Perform quarterly Privileged Account reviews.
        - Perform quarterly Separated User reviews.
        - Perform monthly Inactive Account Reviews

## 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*

Mailing Address, Residential Address, Zip Code, Phone Numbers, Email Address, Race, Ethnicity, Military History, Veteran Interactions.

**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 https://www.archives.gov/records-mgmt/grs? 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 5.2, item 020. Item 020 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 (Frequently Asked Questions about GRS 5.2, Transitory and Intermediary Records | National Archives).

**3.3 The retention schedule 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. Please work with the system 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?*

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 5.2, item 020. Item 020 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 (Frequently Asked Questions about GRS 5.2, Transitory and Intermediary Records | National Archives).

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

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 5.2, item 020. Item 020 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 (Frequently Asked Questions about GRS 5.2, Transitory and Intermediary Records | National Archives). Disposition Instruction: Temporary, Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later. DAA-GRS-2022-0009-0002

### 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.*

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. 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 (including Pre-Production and Data Quality 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 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 Privacy Officer (PO) 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:* *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

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

Follow the format below:

**Privacy Risk:** There is a risk that the information maintained by 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.

**Mitigation:** 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.

**PII Mapping of Components**

4.1a **VA Profile** consists of <**number**> 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 **VA Profile** and the reasons for the collection of the PII are in the table below.

**Note**: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

*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** |
|---|---|---|---|---|---|
| VA PROFILE: (Instance 1) | **No** | **Yes** | • Personal Address, Phone & Email | Storage of PII to enable partner systems to utilize | VA Profile uses FIPS validated encryption |

| | | | | | |
|---|---|---|---|---|---|
| | | | • Race, Ethnicity<br>• Veteran Interactions<br>ICN, First Name, Last Name, SSAN, DOB, Mothers Maiden, Place of Birth, Gender | authoritative contact data source.<br>**Data used to determine Identity.** | in the transfer and storage of PII. |
| VBA Corporate Database: (Instance 1) | **Yes** | **Yes** | • Contact Info(Emails, Addresses, Phones)<br>• Person Attributes (Fiduciary, Fraud Indicators)<br>• Disability Ratings<br>• Awards<br>Correlated Identifiers (PID) | Contact Info(Emails, Addresses, Phones)<br>Person Attributes (Fiduciary, Fraud Indicators) | CRP has ATO's in place that establishes their safeguards.<br>Benefits Application Infrastructure - 1373<br>VBACorporate Infrastructure-129 |
| VADIR: (Instance 1) | **Yes** | **Yes** | • Personal Address, Phone & Email<br>Military History, Race, Ethnicity | 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 | VADIR has an ATO in place that establishes their safeguards.<br>VA DoD Identity Repository - 126 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | approximately 13 million Veterans. | |
| CDW | **Yes** | **Yes** | Contact Info(Emails, Addresses, Phones) Military Personnel Data ( Service Summary Code (SSC))<br>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, 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. | CDW has ATO's in place that establishes their safeguards. CDCO-AITC-VHA-CDW Assessing - 139<br>CDW in Azure - 944 |
| CXI | | | - Personal Address, Phone & Email | Customer Experience Data Warehouse (CxDW) (AKA | CxDW has an ATO in place that establishes |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
|  |  |  | • Interaction History (Names, relationships, and Call logs from various CRMs)<br>VA Profile Transaction History Logs (that may contain PII/PHI from other sources) | CxI) 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. | their safeguards.<br>Summit Data Platform |
| HDR | **Yes** | **Yes** | PHI – Active Prescription Records, used to determine if Contact Information updates can be made without impacting critical medication delivery. | The Health Data Repository II (HDR II) is a data repository of clinical information that resides on one or more independent 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 | HDR II has an ATO in place that establishes their safeguards.<br>Health Data Repository - 113 |

| | | | | | |
|---|---|---|---|---|---|
| | | | | 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 | |
| MPI: Server 1, Server 2, Server 3, Server 4, Server 5 | **Yes** | **Yes** | • Correlated Identifiers (examples: EDIPI, ICN, PID, ESR, PID, VHIC ID, etc.)<br>• Legal Name (Surname, First Name, Middle Name, Prefix, Suffix, Preferred)<br>• Preferred Name<br>• Alias<br>• Date of Birth<br>• Place of Birth (City, State, Province, Country)<br>• Multiple Birth (Indicator, Birth Order) | MPI is the Authoritative Source in VA for Identity and it maintains the list traits used to determine Identity and provides the list of correlated ID's across other VA Systems. | MPI has an ATO in place that establishes their safeguards. |

| | | | | | |
|---|---|---|---|---|---|
| | | | • Social Security Number (SSN)<br>• Date of Death (Date, Indicator, Last Updated, Entered By, Last Edited By, Supporting Document Type, Source of Notification, Option Used, Override Reason)<br>• Birth Sex<br>• Admin Sex<br>• Gender Identity<br>• Pronoun<br>• Sexual Orientation<br>• Mother's Maiden Name<br>• Assigning Location<br>• Person Type<br>Relationships | | |

**4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.**

**NOTE: Question 3.9b (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*

| ***IT system and/or Program office. Information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List PII/PHI data elements shared/received/transmitted.*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| (VBMS) Veterans Benefits Management System | Contact Information Services, Demographics | • Personal Address, Phone & Email<br>• Race, Ethnicity<br>Correlated Identifiers | RESTful (Representational state transfer) Web Service Using HTTPS (Hypertext Transfer Protocol Secure) with MTLS (Mutual Transport Layer Security) |
| Corporate Database | Contact Information Services, Communication Permissions, Disability Ratings Services, Awards Services, Indicators | • Personal Address, Phone & Email<br>• Financial Info, Medical History<br>• Correlated Identifiers | 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 |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
|  |  |  | HTTPS (Hypertext Transfer Protocol Secure) (one-way) |
| Benefit Gateway Services (BGS) | Contact Information Services, Indicators | • Financial Info, Medical History<br>• Service Connection/Disability Financial<br>• Admin Decisions, Military Service<br>Correlated Identifiers | SOAP (Simple Object Access Protocol) Web Service Using HTTPS (Hypertext Transfer Protocol Secure) with MTLS (Mutual Transport Layer Security) |
| Benefits Integration Platform (BIP) | Contact Information Services, Disability Ratings Services, Awards Services | • Financial Info, Medical History<br>• Service Connection/Disability Financial<br>Correlated Identifiers | SOAP (Simple Object Access Protocol) Web Service Using HTTPS (Hypertext Transfer Protocol Secure) with MTLS (Mutual Transport Layer Security) |
| Electronic Virtual Assistant<br>(e-VA) | Contact Information Services | • Personal Address, Phone & Email<br>• Correlated Identifiers | REST (Representational state transfer) (GET, PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| | | | Transport Layer Security) |
| Readiness and Employment System (RES) | Contact Information Services, Demographics, Military Service Data, Disability Ratings Services, Awards Services, Indicators | • Financial Info, Medical History<br>• Service Connection/Disability<br>• Personal Address, Phone & Email<br>• Race, Ethnicity<br>• Military History<br>• Financial Correlated Identifiers | REST (Representational state transfer) (GET, PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security) |
| Life Insurance Policy Administration Solution (LIPAS) | Contact Information Services, Disability Ratings Services, Awards Services | • Personal Address, Phone & Email<br>• Service Connection/Disability<br>• Correlated Identifiers | REST (Representational state transfer) (GET, PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security) |
| Electronic Insurance (EIN) | Disability Ratings Services | • Service Connection/Disability<br>• Correlated Identifiers | REST (Representational state transfer) (GET, PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security) |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| Customer Relationship Management Unified Desktop Optimization (CRM UD-O) | Contact Information Services, Military Service Data, Interaction History | • Personal Address, Phone & Email (Future)<br>• Customer Interaction (Future)<br>• Military History (Future)<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Visitor Outreach Interaction and Communication Engine (VOICE) Replacing CRM UD-O | Contact Information Services, Military Service Data, Interaction History | • Personal Address, Phone & Email (Future)<br>• Customer Interaction (Future)<br>• Military History (Future)<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| VCIP Source Material Tracking (VCIP SMTS) QUICKSUBMIT | Contact Information Services, Communication Permissions | • Personal Address, Phone & Email<br>• Communication Permissions<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Digital GI Bill (DGIB) | Contact Information Services, Demographics, Military Service Data, Health Benefits, Disability Ratings Services, Awards Services | • Personal Address, Phone & Email<br>• Financial Info, Medical History, (Future)<br>• Service Connection/Disability (Future)<br>• Race, Ethnicity (Future)<br>• Military History (Future)<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |

| ***IT system and/or Program office. Information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List PII/PHI data elements shared/received/transmitted.*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| Federal Case Management Tool (FCMT) | Contact Information Services, Demographics, Military Service Data | • Personal Address, Phone & Email<br>• Race, Ethnicity<br>• Military History<br>Correlated Identifiers | |
| Loan Guaranty (LGY) | Contact Information Services | • Personal Address, Phone & Email<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Salesforce Veteran Home Benefit (VHB) | Contact Information Services, Demographics, Military Service Data, Health Benefits, Disability Ratings Services, Awards Services, Indicators | • Financial Info, Medical History (Future)<br>• Personal Address, Phone & Email (Future)<br>• Race, Ethnicity (Future)<br>• Service Connection/Disability (Future)<br>• Military History (Future)<br>• Ratings (Future)<br>• Financial Info, Medical History (Future)<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Status Query and Response Exchange (SQUARES) | Contact Information Services, Demographics, Military Service Data, Health Benefits, | • Personal Address, Phone & Email<br>• Race, Ethnicity<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| | Disability Ratings Services, Awards Services | Medical Record Numbers<br>• Military History<br>Correlated Identifiers | |
| Enrollment System (VES) -<br>(ADS - Health Eligibility) | Contact Information Services, Demographics, Military Service Data, Health Benefits, Disability Ratings Services, Awards Services | • Financial Info, Medical History<br>• Personal Address, Phone & Email<br>• Race, Ethnicity<br>• Service Connection/Disability<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers<br>• Military History<br>Correlated Identifiers | SOAP (Simple Object Access Protocol) Web Service Using HTTPS (Hypertext Transfer Protocol Secure) with MTLS (Mutual Transport Layer Security)<br>REST (Representational state transfer) (GET, PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security) |
| Caregiver Record Management Application (CARMA) | Contact Information Services, Demographics, Military Service Data, Health Benefits, Disability Ratings Services, | • Personal Address, Phone & Email<br>• Race, Ethnicity<br>• Military History<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| | Awards Services, Indicators | Numbers Service Connection/Disability<br>• Financial, Medications, Medical Records<br>Correlated Identifiers | |
| Member Services - Customer Relationship Management (MS CRM) | Contact Information Services, Interaction History | • Personal Address, Phone & Email (Future)<br>• Interaction History (Future)<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Health Data Repository (HDR II) (ADS – Prescription) | Health Benefits, Indicators | • Prescription Information<br>Correlated Identifiers | SOAP (Simple Object Access Protocol) Web Service Using HTTPS (Hypertext Transfer Protocol Secure) with MTLS (Mutual Transport Layer Security) |
| My HealtheVet (MHV) | Contact Information Services, Communication Permissions, Demographics, Military Service Data, Health Benefits | • Military History<br>• Personal Address, Phone & Email (Future)<br>• Race, Ethnicity (Future)<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers (Future)<br>Correlated Identifiers | REST (Representational state transfer) (GET, PUT and POST) over HTTPS (Hypertext Transfer Protocol Secure) using MTLS (Mutual Transport Layer Security) |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| Veterans Integrated Registries Platform (VIRP) | Contact Information Services, Demographics, Military Service Data | - Personal Address, Phone & Email<br>- Race, Ethnicity<br>- Military History<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| WellHive Advanced Medical Cost Management System (WellHive AMCMS ) | Contact Information Services | - Personal Address, Phone & Email<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Integrated Scheduling Solution (ISS) | Contact Information Services, Demographics, Health Benefits, Disability Ratings Services, Awards Services | - Personal Address, Phone & Email<br>- Race, Ethnicity<br>- Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers<br>- Service Connection/Disability<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Check-in Experience (CIE) | Contact Information Services, Health Benefits | - Personal Address, Phone & Email (Future)<br>- Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers (Future)<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| CPAP Reporting (Somnoware) - | Contact Information Services, | - Personal Address, Phone & Email<br>- Medical Records, | RESTful Web Service Using HTTPS with |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| | Health Benefits, Disability Ratings Services, Awards Services | Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers<br>• Service Connection/Disability<br>Correlated Identifiers | MTLS (Mutual Transport Layer Security) |
| VA Health Connect Customer Relationship Management (VAHC CRM) | Contact Information Services, Health Benefits, Indicators | • Personal Address, Phone & Email<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers<br>• Financial, Medications, Medical Records<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Data and Analytical Support for Healthcare (DASH) | Disability Ratings Services, Awards Services | • Service Connection/Disability<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Joint Electronic Health Record System (CM) | Contact Information Services, Demographics, Health Benefits | • Personal Address, Phone & Email<br>• Race, Ethnicity<br>• Service Connection/Disability<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| | | Numbers<br>Correlated Identifiers | |
| Veteran Facing Services Platform (Vets.gov)<br>VA.gov<br>VA Notify | Contact Information Services, Communication Permissions, Demographics, Military Service Data, Health Benefits, Gender Identity, Indicators | • Personal Address, Phone & Email<br>• Race, Ethnicity<br>• Military History<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers, Gender<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| VA/DoD Identity Repository (VADIR) | Contact Information Services, Demographics, Military Service Data | • Personal Address, Phone & Email<br>• Race, Ethnicity<br>• Military History<br>Correlated Identifiers | Oracle GoldenGate Using TCPS (Transfer Control Protocol with SSL) |
| VA Master Person Index (VA MPI) | Contact Information Services, Demographics, Military Service Data, Health Benefits, Gender Identity | • Personal Address, Phone & Email<br>• Financial, Medications, Medical Records<br>• Race, Ethnicity<br>• Personal Traits<br>• Person Identity (Future)<br>o Correlated Identifiers (examples: EDIPI, ICN, PID, ESR, PID, VHIC ID, etc.)<br>o Legal Name (Surname, First Name, Middle Name, Prefix, | SOAP (Simple Object Access Protocol) Web Service Using HTTPS (Hypertext Transfer Protocol Secure) with MTLS (Mutual Transport Layer Security) |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| | | Suffix, Preferred)<br>○ Preferred Name<br>○ Alias<br>○ Date of Birth<br>○ Place of Birth (City, State, Province, Country)<br>○ Multiple Birth (Indicator, Birth Order)<br>○ Social Security Number (SSN)<br>○ Date of Death (Date, Indicator, Last Updated, Entered By, Last Edited By, Supporting Document Type, Source of Notification, Option Used, Override Reason)<br>○ Birth Sex<br>○ Admin Sex<br>○ Gender Identity<br>○ Pronoun<br>○ Sexual Orientation<br>○ Mother's Maiden Name<br>○ Assigning Location<br>○ Person Type<br>Relationships | |
| VA Customer Experience Service Recovery Platform | Contact Information Services, Indicators | • Personal Address, Phone & Email | RESTful Web Service Using HTTPS with |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| (VA CX SRP) | | • Financial, Medications, Medical Records<br>Correlated Identifiers | MTLS (Mutual Transport Layer Security) |
| Veterans Identification Card (VIC) | Contact Information Services, Military Service Data | • Personal Address, Phone & Email<br>• Military History<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Enterprise Veterans Self Service (EVSS) | Contact Information Services | • Personal Address, Phone & Email<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Solution (VEIS) (Gateway) | Contact Information Services, Interaction History, Demographics, Military Service Data, Health Benefits, Disability Ratings Services, Awards Services, Gender Identity, Indicators | • Financial Info, Medical History<br>• Personal Address, Phone & Email<br>• Customer Interaction (Future)<br>• Race, Ethnicity<br>• Service Connection/Disability Gender<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers Military History<br>• Financial, Medications, Medical Records<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| Patient Advocate Tracking System Replacement (PATS-R) | Contact Information Services, Demographics, Interaction History | • Personal Address, Phone & Email (Future)<br>• Customer Interaction (Future)<br>• Race, Ethnicity<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Veteran Exposure Team-Health Outcomes Military Exposures (VetHome) | Contact Information Services, Military Service Data, Health Benefits, Disability Ratings Services, Awards Services, Indicators | • Personal Address, Phone & Email<br>• Service Connection/Disability Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers<br>• Military History<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Salesforce: Medical Foster Homes (SF-MFH) | Contact Information Services, Disability Ratings Services | • Personal Address, Phone & Email<br>• Race, Ethnicity<br>• Service Connection/Disability<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Community Care - Customer Relationship Management (CommCare-CRM) | Contact Information Services, Demographics, Military Service Data, Health Benefits, Disability Ratings Services, | • Personal Address, Phone & Email<br>• Race, Ethnicity<br>• Service Connection/Disability Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| | Awards Services | Correlated Identifiers | |
| Mobile Application Platform (MAP)<br>Includes:<br>Mental Health Checkup (MHCHECKUP)<br>Virtual Care Manager (VCM)<br>Annie,<br>Virtual Shares Services (VSS) | Contact Information Services, Demographics, Health Benefits, Disability Ratings Services, Awards Services, Indicators | • Personal Address, Phone & Email<br>• Race, Ethnicity<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers<br>• Service Connection/Disability<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Digital Veterans Platform (DVP)<br>Lighthouse Eligibility APIs (LHELG) - #3299<br>Includes:<br>FCC Lifeline Program API<br>Letter Generator API Includes EVSS<br>Veteran Confirmation API<br>Multiple External<br>Veteran Verification API<br>SYNC.MD<br>COMBINEDARMS<br>WOUNDEDWARRIOR | Contact Information Services, Military Service Data, Disability Ratings Services, Awards Services, Gender Identity, Indicators | Correlated Identifiers - All<br>• Financial Info, Medical History<br>• Personal Address, Phone & Email<br>• Military History | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| DTC Integration Platform (DIP) | Contact Information Services, | • Personal Address, Phone & Email<br>• Race, Ethnicity | RESTful Web Service Using HTTPS with |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| | Demographics, Military Service Data, Health Benefits, Disability Ratings Services, Awards Services, Gender Identity, Indicators | • Military History<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers<br>• Service Connection/Disability<br>• Financial, Medications, Medical Records<br>Correlated Identifiers | MTLS (Mutual Transport Layer Security) |
| VEText (Text Message Appointment Reminders) (VEText) | Contact Information Services, Communication Permissions | • Personal Address, Phone & Email<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Veteran Account Management System Debt Management Center | Contact Information Services, Health Benefits, Disability Ratings Services, Awards Indicators | • Personal Address, Phone & Email<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers<br>• Service Connection/Disability<br>• Financial, Medical Records<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Salesforce - Grants4Vets (SF-NVSPSE) | Health Benefits | • Medical Records, Emergency Contact Information, Next of Kin, Health Insurance | RESTful Web Service Using HTTPS with MTLS (Mutual |

| ***IT system and/or Program office. Information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List PII/PHI data elements shared/received/transmitted.*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| | | Beneficiary Numbers, Medical Record Numbers<br>Correlated Identifiers | Transport Layer Security) |
| Salesforce - Veteran Outreach for VA Vet Centers Readjustment Counseling<br>(SF VetOutreach) | Contact Information Services, Military Service Data, Disability Ratings Services, Indicators | • Personal Address, Phone & Email<br>• Service Connection/Disability<br>• Military Service<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| Pega - Electronic Dental Eligibility Verification Solution (Pega-EDEVS) | Military Service Data, Health Benefits, Disability Ratings Services, Awards Services, Indicators | • Military History<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers<br>• Service Connection/Disability<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |
| External Data Transfer System (EDTS) Component: Virtual Care Clinic | Contact Information Services, Military Service Data, Health Benefits | • Personal Address, Phone & Email (Future)<br>• Military History (Future)<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers (Future)<br>Correlated Identifiers | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |

| *IT system and/or Program office. Information is shared/received with* | *List the purpose of the information being shared /received with the specified program office or IT system* | *List PII/PHI data elements shared/received/transmitted.* | *Describe the method of transmittal* |
|---|---|---|---|
| Telehealth Management Platform (TMP/CVT-TSS) | Contact Information Services, Military Service Data, Health Benefits | • Personal Address, Phone & Email (Future)<br>• Military History (Future)<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance Beneficiary Numbers, Medical Record Numbers (Future)<br>Correlated Identifiers | RESTful Web Service Using HTTPS with 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 VA network 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 in this section.).*

*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.

**<u>Mitigation:</u>** 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.**

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

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

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

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

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

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

*Data Shared with External Organizations*

| ***List IT System or External Program Office information is shared/received with*** | ***List the purpose of information being shared / received / transmitted*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted)*** | ***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*** | ***List the method of transmission and the measures in place to secure data*** |
|---|---|---|---|---|
| Joint Health Information Exchange (JHIE) (External System) | Provide Patient Contact and Related Care information for use in Joint VA/DoD | • Personal Address, Phone & Email<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance, Beneficiary Numbers, Medical Record Numbers<br>• Service Connection/Disability<br>Correlated Identifiers | National ISA/MOU | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |

| | | | | |
|---|---|---|---|---|
| | Medical Facilities | | | |
| Joint Electronic Health Record System (JEHRS) | Provide Patient Contact and Related Care information for use in Joint VA/DoD Medical Facilities | • Personal Address, Phone & Email<br>• Medical Records, Emergency Contact Information, Next of Kin, Health Insurance, Beneficiary Numbers, Medical Record Numbers<br>• Service Connection/Disability<br>Correlated Identifiers | National ISA/MOU | RESTful Web Service Using HTTPS with MTLS (Mutual Transport Layer Security) |

### 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:** 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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.**

*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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.*

VA Profile does not directly collect the information, the source systems that perform this function including VA.gov document this function within their Boundaries and Documentation.

*6.1b If notice was not provided, explain why.*

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 October 23, 2023. Please Reference 88 FR 72820 and SORN # 192VA30.

*6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.*

VA Profile does not directly collect the information, the source systems that perform this function including VA.gov document this function within their Boundaries and Documentation.

**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 directly collect the information, the source systems that perform this function including VA.gov document this function within their Boundaries and Documentation.

**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 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.

**6.4 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 Privacy Officer (PO) 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:* *This is referring to sufficient notice provided to the individual.*

*Principle of Use Limitation:* *The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 # 192VA30 and publication of 88 FR 72820 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 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 [VA Public Access Link-Home (efoia-host.com)](efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

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.

*7.1b 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)?*

No exemption.

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

The system is subject to Privacy Act as documented in 7.1a.

**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.* ***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.*

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 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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

*Consider the following FIPPs below to assist in providing a response:*
*Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.*

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

*Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.*
*This question is related to privacy control IP-3, Redress.*

Follow the format below:

**Privacy Risk:** There is a risk that the information provided to VA Profile is inaccurate and decisions are made with incorrect information.

**Mitigation:** 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. (Work with your ISSO to complete this section).

**8.1 The procedures in place to determine which users may access the system, must be 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?*

VA Profile functions as a back-end system. 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.

*8.1b 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?*

VA Profile functions as a back-end system. 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. **No users from other agencies have direct access to VA Profile data**.

*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.*

VA Profile supports roles to permit Read, Write and Subscribe by partner applications. Permissions are granted to the System and those systems carry the responsibility of access control within their boundary.

**8.2a. Will VA contractors have access to the system and the PII?**

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.

**8.2b. What involvement will contractors have with the design and maintenance of the system?**

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.

**8.2c. Does the contractor have a signed confidentiality agreement?**

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.

**8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?**

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.

**8.2e. Does the contractor have a signed non-Disclosure Agreement in place?**
*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.*

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 The Authorization and Accreditation (A&A) completed for the system.**

*8.4a If Yes, provide:*

1. *The Security Plan Status:* **APPROVED**
2. *The System Security Plan Status Date:***05-Sep-2024**
3. *The Authorization Status:* **Authorization to Operate (ATO)**
4. *The Authorization Date:* **16-Dec-2024**
5. *The Authorization Termination Date:* **15-Dec-2025**
6. *The Risk Review Completion Date:* **09-Oct-2024**
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.*

*8.4b 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, 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.* ***(Refer to question 1.8 of the PTA)***

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

**9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

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

**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.*

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

**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.*

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

**9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.**

*Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).*

The system does not 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** |
| 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.**

ANMAR FAIK Digitally signed by ANMAR FAIK
Date: 2025.01.13 13:26:04
-05'00'

**Privacy Officer, Anmar Faik**

CLYDE JOHNSON Digitally signed by CLYDE JOHNSON
Date: 2025.01.13 13:56:38
-05'00'

**Information Systems Security Officer, Clyde "Butch" Johnson**

FRED SPENCE Digitally signed by FRED SPENCE
Date: 2025.01.13 13:55:20 -06'00'

**Information Systems 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; screen shot of a website collection privacy notice).

## HELPFUL LINKS:

**Records Control Schedule 10-1 (va.gov)**

**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 Directive 1605.04
IB 10-163p (va.gov)