Privacy Impact Assessment for the VA IT System called:

Identity and Access Management (IAM)

VHA

IAM Business Program Office; Infrastructure Operations (IO)

Date PIA submitted for review:

9/26/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Wade Stromer	Wade.Stromer@va.gov	307-461-0180
Information System Owner	Kevin Willis	Kevin.Willis10@va.gov	352-207-8483

Abstract

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

Identity and Access Management (IAM) is a cloud-based collection of interconnected applications to provide access and identity services to VA Employees, Contractors, Veterans, volunteers, clinical trainees and external partners. These IAM services will enable all persons of interest to VA, which include internal VA Users and potential external population that include but are not limited to all Veterans, Beneficiaries and Business Partners, to find uniform information about VA's benefits and services regardless of access channel to all individuals to complete their transactions within VA; be identified quickly by VA, without having to repeat information; and seamlessly access multiple VA service lines. These IAM services will enable all persons of interest to VA, which include internal VA Users and potential external population that include but are not limited to all Veterans, Beneficiaries and Business Partners, to find uniform information about VA's benefits and services regardless of access channel to all individuals to complete their transactions within VA; be identified quickly by VA, without having to repeat information; and seamlessly access multiple VA service lines. Identity and Access Management (IAM) is a cloud-based collection of interconnected applications to provide access and identity services to VA Employees, Contractors, Veterans, volunteers, clinical trainees, and external partners.

Overview

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

1 *General Description*

A. *The IT system name and the name of the program office that owns the IT system.*

IAM is a major application under the control of the Veterans Administration Cloud (VAEC) and the Infrastructure Operations office (IO)

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

IAM is a major application under the control of the Veterans Administration Cloud (VAEC) and the Infrastructure Operations office (IO) and consist of a suite of applications that provides cloud-based enterprise authentication and identity services for the entire Veteran population, all non-organizational and organizational user to VA systems. IAM provides PIV authentication to over 400 internal VA applications and some specific external users (such as individuals with ID.me that are outside of the VA network) to get access to resources, benefit and health information. IAM provides a set of processes and technologies to manage identities across multiple systems, encompassing identity (based on an identifier and a set of attributes) and access (interactions with information and other assets). These processes may be based on individual users, roles, or organizations. The IAM serves approximately 950 other systems in VA in the form of verification of identity; this number changes as new systems adopt IAM for authentication and other systems are decommissioned. Each user session is encrypted and isolated from all other sessions to maintain confidentiality, integrity, and privacy. VA technology system end users (both internal and external) currently must maintain multiple user Identification (ID)/Password combinations to access all VA resources for which they have been granted permissions. Electronic submission of VA claims forms requires digital signature capabilities. Veteran satisfaction and ease of access to benefits-services will be improved.IAM systems verify credential and collect audit logs based on access requested and contains PII that might have been captured into order to authenticate to the resource. IAM corelates information from the MPI. Master Person Index which has over 1 million Veteran records. Veteran Health Identification Card (VHIC) system users capture Veteran PII in order to provide access to health benefit card and may capture PII related to granting to those request and audit data related to those actions MPI is the system responsible for Identity Management and consists of Person Services (PSIM) and Master Patient Index. (MPI) Person Services Identity Management (PSIM), consists of Identity Management Data Quality (IMDQ) Toolkit (TK) and Master Data Management (MDM) which was formerly IdentityHub (IdHub). MDM is a Commercial off-the-shelf (COTS) software package configured with a custom VA-specific probabilistic algorithm for identifying and scoring persons. PSIM and IMDQ Toolkit are custom built for the VA. There are up to 50 verified users however the main interactions are from other applications. Over three dozen applications connect directly and around 700 applications connect indirectly to query regarding identities via PSIM as the authoritative source. PSIM allows client applications to access person records of all categories. (This allows for one connection to the database which is used by numerous applications rather than numerous connections to the database.) Toolkit (TK) is a web-based GUI used to optimize Identity Resolution workflow, allowing for quick resolution of duplicates, improved data matching and identification of new possible duplicates or mismatches. The GUI allows viewing, tracking and updating all MPI identities as well as providing remote data views into the correlated systems to aid in the manual matching of the disparate systems identities. MDM is an advanced search software for duplicate reduction based on scoring of account profiles. Searches in MDM are executed by PSIM. If some data is known for a veteran, the known fields are input and MDM searches the entire veteran listing and returns the closest match.

C. *Indicate the ownership or control of the IT system or project.*

IAM is a major application under the control of the Veterans Administration Cloud (VAEC) and the Infrastructure Operations office (IO)

2. Information Collection and Sharing

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

The expected number of individuals whose information is stored in the system is over a million and the typical clients or affected individuals are VA employees and contractors.

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

IAM provides PIV authentication to over 400 internal VA applications and some specific external users (such as individuals with ID.me that are outside of the VA network) to get access to resources, benefit and health information. IAM provides a set of processes and technologies to manage identities across multiple systems, encompassing identity (based on an identifier and a set of attributes) and access (interactions with information and other assets).

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

The modules and subsystems, where relevant, and their functions include: • Single Sign On internal is used to provide PIV card identification to VA applications. • Single Sign On external is used to provide credential access to VA applications • Provisioning allows external application owners to assign access permissions. • Security Token Service • Authorization Management Service references other components of the system to authorize the use of partner applications and veterans• Credential Service Provider is the local PIV credential service provider used to verify access when using PIV credentials. • Electronic Signature provides digital signature services to customer applications. • Compliance Auditing and Reporting collects audit records of action on the system (e.g. user logons) and provides reports of record metrics. • Manages and correlates the ability to uniquely identify a person and the facilities where that person receives care is a key asset in the delivery of quality care System use resources through VA Enterprise Architecture such as Master Veterans Index (MPI), Active Directory (AD) and Certificate Authority (CA)

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

The system is managed as a major application under VAEC cloud. CSP does not have access to IAM information. The relationship between VA and CSP falls under the responsibility of VAEC team, and furthermore the CSP does not have access to VA data on IAM. The MS Azure Government has environment has been certified by the VA and approved to house applications with a FIPS 199 categorization of HIGH. MS Azure has a ATO signed and expires January 14, 2024 and has FedRamp High certification.MS Azure Government personnel are responsible for the secure configuration, maintenance, and monitoring of physical environment. MS Azure Government is a component of VA Enterprise Cloud Services. MS Azure is separate from VA network and accessed through TIC Trusted Internet Connection maintained by VA National Security Operations Center (NSOC) VA NSOC monitors and controls all access and transmissions through Azure. VA NSOC makes an IPSEC VPN TIC Compliant connection to the MS Azure Infrastructure As A Service (IaaS) environment. VA NSOC has control over both ends points of the VPN environment.

3. Legal Authority and SORN

H. *A citation of the legal authority to operate the IT system.*

Legal authorities are Title 38, United States Code, Section 501 – Veterans' Benefits and Joint Commission National Patient Safety Goals – Identify patients correctly The following is a full list of related laws, regulations and policies and the legal authorities: NIST Special Publication 800-63 Version 1.0.2; Electronic Authentication Guideline OASIS XACML 2.0 Section 508 Standards Guide VA Directive 6500; Information Security Program VA Directive 6501; VA Identity Verification World Wide Web Consortium (W3C) SOAP Standard World Wide Web Consortium (W3C) XML Standard FICAM Roadmap and Implementation Guidance OMB 04-04 E-Authentication Guidance for Federal Agencies Aligns with the VA Enterprise Shared Services directive and strategy Supports HSPD-12 specifications where applicable (i.e., Personal Identification Verification (PIV)) Title 38, U.S.C. Chapter 3, Section 210 (c) (1), Title 38 U.S.C. 7301, 5 U.S.C. 552a.and Executive order 9397. • 150VA19 – Privacy Act, authority to use/collect SSN• 138VA005Q – Privacy Act, authority to use/collect SSN• System of Records 121VA10A7 – National Patient Databases-VA • System of Records 24VA10A7 – Patient Medical Records-VA • Title 38, United States Code, Section 501 – Veterans' Benefits • Joint Commission National Patient Safety Goals – Goal 1: Improve the accuracy of patient Identification Enterprise

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

No major changes were made, or modifications planned within the period of the PIA timeframe. No SORNs will need amendment or revision. All applicable SORNs utilized should cover IAM instance within the VAEC environment.

D. System Changes

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

No. Completion of PIA will not require any changes to the IAM environment or processes.

K. Whether the completion of this PIA could potentially result in technology changes

No. Completion of PIA will not require any changes to the IAM technological environment.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Information in table and below is collected in form VA 10-10EZ in order to enroll Veterans into VA health care system. The information provided on this form will be used by VA to determine your eligibility for medical benefits. No data is retained by IAM other than what is captured in audit log files.
UserID, eAL1, eAL2, eAL3, eAL4 (Electronic Authentication Assurance Level), Authentication Tokens; password, PIN, Public Key Infrastructure (PKI) on Smart Card, Soft Certificate, Gender, Military Service Record

MPI data retained
Integration Control Number (ICN), Surname, First Name, Middle Name, Name Prefix, Name Suffix, Mother's Maiden Name, Date of Birth, Place of Birth City (POBC), Place of Birth State (POBS), Date of Death, Death Verification Status, Gender, Social Security Number (SSN), SSN Verification Status, Pseudo SSN Reason, Coordinating Master of Record, Sensitivity, Primary ICN, Date/Time of Original Creation, Facility of Original Creation, Created By, Resolution Journal Case Number, Primary View Date Last Updated, Identity Theft, Temporary ID Number, Foreign ID Number, Street Address [Line 1], Street Address [Line 2], Street Address [Line 3], City [Residence], State [Residence], Zip+4 [Residence], Phone Number [Residence], Multiple Birth Indicator, Province Postal Code, Country, Alias, Alias Surname, Alias First Name, Alias Middle Name, Alias Prefix, Alias Suffix, Alias SSN, Alias Date Last Updated, Race Information, Race Date Last Updated, Ethnicity Information, Ethnicity Date Last Updated, ID State, Date of ID State, Surname Primary View Score, First Name Primary View Score, Middle Name Primary View Score, Prefix Primary View Score, Suffix Primary View Score, DOB Primary View Score, Gender Primary View Score, SSN Primary View Score, MMN Primary View Score, Mult Birth Primary View Score, POB City Primary View Score, POB State Primary View Score.

PII Mapping of Components (Servers/Database)

Identity and Access Management consists of 42 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Identity and Access Management and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
mdbs175	Yes	Yes	May include: Name, DOB, SSN, Mothers’	PII associated to user profiles	Data at rest and in transit is

			Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	that is used to verify identity	encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
mdbs176	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-mpdb125	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated

			Address, Home Phone,		privileges are granted access in accordance with NIST and VA policy.
TX-mpdb126	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
mpdb128	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-mdbs175	Yes	Yes	May include: Name, DOB,	PII associated to user profiles	Data at rest and in

			SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	that is used to verify identity	transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-mdbs176	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
mpdb125	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with

			Correspondence Address, Home Phone,		elevated privileges are granted access in accordance with NIST and VA policy.
mpdb126	Yes	Yes	May include: Name, DOB, SSN, Mothers’ Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
mpdb325	Yes	Yes	May include: Name, DOB, SSN, Mothers’ Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.

mpdb326	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
MDBS100	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
MDBS101	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only

			Alias Name and SSN, Correspondence Address, Home Phone,		personnel with elevated privileges are granted access in accordance with NIST and VA policy.
MDBS102	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
MMDB335	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST

					and VA policy.
TX-MMDB135	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-MMDB136	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-MMDB137	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in

			Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,		place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-mdbs375	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX- mdbs376	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance

					with NIST and VA policy.
mdbs375	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
mdbs376	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-mpdb326	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical

			Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,		access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-mpdb325	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-MDBS300	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in

					accordance with NIST and VA policy.
TX-MDBS301	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-MDBS302	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
MDBS300	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and

			Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,		logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
MDBS301	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
MDBS302	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted

					access in accordance with NIST and VA policy.
TX-MMDB335	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-MMDB336	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-MMDB337	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted;

			Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,		Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
MMDB336	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
MMDB337	Yes	*Yes*	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges

			Address, Home Phone,		are granted access in accordance with NIST and VA policy.
TX-mpdb128	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-MDBS100	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-MDBS101	Yes	Yes	May include: Name, DOB, SSN, Mothers'	PII associated to user profiles	Data at rest and in transit is

			Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	that is used to verify identity	encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
TX-MDBS102	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
MMDB135	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated

			Address, Home Phone,		privileges are granted access in accordance with NIST and VA policy.
MMDB136	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.
MMDB137	Yes	Yes	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone,	PII associated to user profiles that is used to verify identity	Data at rest and in transit is encrypted; Physical and logical access in place to ensure only personnel with elevated privileges are granted access in accordance with NIST and VA policy.

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Identity and Access Management correlates data, to include PII, from the Master Veterans Index (MPI). The data from IAM is derived from internal and external sources to VA. IAM does not capture any data except at the terminals for Veterans Health Identification Card, a component of IAM for printing identification cards for Veterans and any data captured at those terminals must all be correlated with other sources of information internal and external to VA. The system checks accuracy against the stored credentials to provide access to VA/ DOD applications. User's information and PII accessed by IAM comes from Credential Service Providers external to the system.

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.

IAM provides internal and external connections to systems allowing single sign on. The sources of data for the external Single sign on component are internal VA applications and external CSP's: Third Party Credential Providers including Defense Manpower Data Center, Norton Single Sign on External) SSO-e) a component of Identify and Access Management (IAM) is application that provides federated identity services allowing veterans or authorized persons of interest to establish a single authenticated identity through a trusted provider (either external or internal to VA), which they can use to access internal VA applications as well applications of other participating government agencies. Multiple internal applications - which are identified and listed in table 4.1- are integrated with SSOe. MPI -No data is collected from sources external to the VA. The MPI is a source of information for numerous systems that verifies the identity of persons in question. In conjunction with the Person Identity Service Management PSIM, MPI forms the Master Person Index (MPI). MPI receives information from the following; • Veterans Information Systems and Technology Architecture (VistA) • Compensation, Pension and Examination (CP&E). MPI is a database that holds millions of unique person identity entries, populated from these Veterans Affairs (VA) line of business; • Veterans Health Administration (VHA). • Veterans Benefits Administration (VBA). • National Cemetery Association (NCA).In conjunction with Master Patient Index (MPI), PSM forms Master Person Index (MPI). MPI is a database that holds millions of unique person identity entries, populated from multiple VA line of businesses (Veterans Health Administration (VHA), Veterans Benefits Administration (VBA) and National Cemetery Association (NCA)). For VHA, information updates can come from Enrollment System Redesign (ESR) or MPI which in turn receives information from VistA as well as Compensation Pension and Examination (CP&E). For VBA, information updates can come from the Beneficiary Identification and Records Locator (BIRLS aka RLS) and VBA C&P Corporate Applications (CRP) databases as well as Vonapp Direct Connect (VDC) Claims processing via eBenefits (EBN) or Digits 2 Digits (D2D) via Stakeholders Enterprise Portal

(SEP). NCA updated information comes to PSM via Burial Operations Support (BOSS)/ Automated Monument Application System (AMAS) (aka MEM). MPI user identity updates can come from Active Directory (AD), VA Person Identification Verification (PIV), USAccess, HRSmart and TMS/EDR.MPI matches/links system records together across the VA systems. The Primary View (PV) profile is considered to be the enterprise "gold copy" of a person's identity record. PV is the best collection of traits known about an Identity among all the sites at the VA where the person has been seen. The PV Profile is referenced in VA information systems by an associated ICN. A Correlation is a person record containing a Source ID and a set of traits as known by the system.The MPI Primary View data traits with ICN includes the fields ICN, ICN Status, Name, SSN, Mother's Maiden Name, SSN Verif Status, Pseudo SSN Reason, Place of Birth City, Place of Birth State, Date of Birth, Multiple Birth Indicator, Alias, ID Theft Flag, Date of Death, Address and Phone Number. This information is shared with systems: Administrative Data Repository (ADR), BizFlow, Enrollment System Redesign (ESR), Health Data Repository (HDR) Clinical Data Service (CDS) and Master Patient Index (MPI). Identity Access Management (IAM) VA Authentication Federation Infrastructure (VAAFI) serves as an intermediary application for numerous systems that connect to query PSM for information. Those systems that connect include: Bidirectional Health Information Exchange (BHIE) Federal Health Information Exchange (FHIE), Bizflow, Beneficiary Identification and Records Locator (BIRLS) (aka RLS), Compensation and Pension Record Interchange (CAPRI), Customer Resource Management (CRM) Unified Desktop (UD), VBA C&P Corporate Applications (CRP), Department of Defense (DoD) Defense Enrollment Eligibility Reporting System (DEERS), eBenefits (EBN), ESR, Experian, Federal Case Management Tool (FCMT), Financial Service Center (FSC), Health Administration Product Enhancements (HAPE), HDR CDS, Health Resource Center (HRC), Health Risk Assessment (HRA), Burial Operations Support (BOSS) Automated Monument Application System (AMAS) (aka MEM), My HealtheVet (MHV), VA Nationwide Health Information Network (NHIN) Gateway Adapter (NHI), (aka eHealth Exchange), Provisioning, Revamp (RVMP), Salesforce, VA Single-sign-on (SSOe), Veterans Benefits Management Systems Assessing (VBMS), Veteran Health Information Card (VHIC), Veterans Profile (VPRF), Vets.gov, Vocational Rehabilitation and Employment (VRE), Vonapp Direct Connect (VDC) Claims Processing and Veterans Information/Eligibility Record Services (VRS, aka VIERS). VRS in turn serves as the communication path through which the Affordable Care Act (ACA) system connects.MPI Correlated IDs includes the fields ID, IDType, Assigning Authority, Assigning Facility and SourceID state. This information is shared with systems: ADR, ESR, MPI. The systems that receive this information via connecting through the intermediary application IAM VAAFI are: BHIE/FHIE, Bizflow, CAPRI, Core Veterans Authorizations and Preferences (NVP, aka VAP) Consumer Preferences and Policy Subsystem (CPP), CRP, Consolidated Registry Service (CRS), EBN, ESR, Experian, FCMT, HDR CDS, HRA, HRC, Janus Joint Legacy Viewer (JLV), BOSS/AMAS (aka MEM), MHV, NHIN Gateway Adapter (NHI) (aka eHealth Exchange), North Chicago Common Registration UI, Core Veterans Authorizations and Preferences (VAP) Consumer Preferences and Policy (CPP) Subsystem (NVP), Provisioning, RLS, RVMP, Salesforce, SSOe, VBMS, VDC, VIC, Vets.gov, VPRF, & VRE.PSM does allow for manual update/override of the MPI Primary View fields based on business review and investigation. The MDM (formerly IdHub) component generates scoring data to allow for match analysis and duplicate reduction.MPI User Identity data includes the following fields pulled from Active Directory, TMS, and/or HRSmart: Name, internal email, external email, required training references, work station#, duty station code, organization code, occupation code, display name, work address, job title, region, contractor company name, supervisor/cor id, sub agency, cost center and key user ids and identity ids (MPI Correlated IDs).IAM Application/system is manually entered as part of an application setup with IAM. The data includes the following fields that Application ID, Approver Groups, Application Roles, Application attributes, Application Roles associated training, Application audit.IAM Provisioning is manually entered or is captured based on an SSO session capture for those applications that are not directly integrated with IAM. The data includes the following fields that User ID, System Approved to access, Approvers of the Access, User Roles, User Application attributes, User Access Status, User Audit.

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

IAM does not create new unique information nor provide reports external to IAM. IAM is not a system of information. Provides authentication and provisioning.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Information for Identity and Access Services is received via electronic transmission from the Master Person Index.SSO-e or VAAFI, a component of Identity and Access Management, does not collect the information on behalf of its users. The system checks accuracy against the stored credentials to provide access to VA/ DOD applications. User's information and PII accessed by VAAFI comes from Credential Service Providers external to the system. User identification information is sent – name, address, phone number, SSN (not sent to all Credential Service Providers), date of birth. Credential Service Provider information cannot be altered by VAAFI users.Third Party Credential Providers including Defense Manpower Data Center, Connect.govMPI-All information is collected using electronic data transfers; all communications are automated using the Heath Level -7 protocol. The Health Level-7 Protocol is the VA-Wide standard used in all communications with the VA VistA. The MPI uses the Health Level-7 Protocol to communicate with the VA VistA.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

No IAM forms or paperwork. IAM does not directly collection any information in paper or physical format.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Information received from MPI is authoritative. All the information will also be checked at the source end. IAM does not collect the information on behalf of its users. The system checks accuracy against the stored credentials to provide access to VA/ DOD applications. User's information and PII accessed by IAM comes from Credential Service Providers external to the system. User identification information is sent – name, address, phone number, SSN (not sent by all CSPs), date of birth. CSP information cannot be altered by VAAFI users. It is externally collected and accessed. Multiple internal applications - which are identified and listed in table 4.1 are integrated with SSO-e component of IAM. Also, Third Party Credential Providers including Defense Manpower Data Center, Connect.gov.For PSM and MPI, business rules and specific field data rules are employed to make sure the data quality is of the best quality. Also, when there are issues, the software pulls the data out to become a manual work item to be reviewed. The manual review is handled by the Identity Management business groups and local Identity Management Points of Contact (POC) via the software. Business rules and specific field data rules are employed to make sure the data quality is of the best quality. When there are issues with data quality the software pulls the data aside to be manually reviewed. The manual review is handled by the Identity Management business groups and local Identity Management Points of Contact via the software. The business rules implemented are requirements for meeting the needs of the VistA

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

No commercial external processes or tool utilized for data integrity. All information is managed within IAM by IAM process and Business rules.

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

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

This system is maintained under the legal authority of Title 38, USC, Section 501 and Section 7304. Identity and Access Management is not a System of Records and the only PII received from the system is data from Master Veterans Index (MPI) which is a System of Record. The MPI System of Record Notice is 24VA10A7 and also System of Records 121VA10A7 – National Patient Databases-VA.

The SORN, 24VA10A7 permits IAM-E correlation of data, to include PII, with the Master Veterans Index (MPI). Additionally, VA internal consuming applications may request specific data from IAM-E services that may include PII

Related to the Privacy Act, SORN 150VA19 (2022) states the records in this system include identifying information including Social Security Number, contact information, educational background, financial information, military service and eligibility information for VHA patients and their providers.

SSO-e or VAAFI, a component of Identity Access Management does not collect the information on behalf of its users. The system checks accuracy against the stored credentials to provide access to VA/ DOD applications. User's information and PII accessed by VAAFI comes from Credential Service Providers external to the system.

There are multiple MOUs for the external Credential Service Providers, and they are listed in the table below. The Privacy Act permits VA to disclose information about individuals without their consent for a routine use when the information will be used for a purpose that is compatible with the purpose for which VA collected the information.

VA 138VA005Q, (Supplementary Information paragraph b, section 2) dated 7/27/2009 permits the collection of information for the application and verification of military benefits for Veterans. DPR 34 allows the collection of PII for the purposes of establishing human resources records.
https://www.oprm.va.gov/privacy/systems_of_records.aspx
http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Article-View/Article/570697/dpr-34- dod/

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: IAM collects both Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation: This system is intended to be used by authorized VA network users for viewing and retrieving information except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA; all use is considered to be understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms. Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties.

Section 2. Uses of the Information

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

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

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

Names, Social Security Number, Phone Number, date of birth, UserID, eAL1, eAL2, eAL3, eAL4 (Electronic Authentication Assurance Level) Authentication Tokens; password, PIN, phone number, PKI on Smart Card, Soft Certificate are used as identifiers in order to authenticate to VA information systems.

Records are captured during the process to apply for a Veterans Health Benefit Card that include: Full Name, DOD Identification Number, Date of Birth, Driver's License Number, Street Address, Email Address, Gender, Home Phone, Photographic Image, Military Service

MPI collects the following data
- Name –Assists in uniquely identifying the person's record.
- Social Security Number (SSN) –Assists in uniquely identifying the person's record.
- Date of birth –Assists in uniquely identifying the person's record.
- Address –Assists in uniquely identifying the person's record.
- Zip code –Assists in uniquely identifying the person's record.
- Phone number –Assists in uniquely identifying the person's record.
- SourceID –Number used to uniquely identify a record. The fully qualified number is unique across all facilities.
- Source –Identifies the system that was the source of the data.
- Integration Control Number (ICN) –Unique VA Identification (ID) number used to bring all separate SourceIDs together across the enterprise.
- ICN status –ID status for the ICN; used to indicate whether the ICN is the current active VA ID or if it has been deactivated. Each deactivated ICN would have a corresponding active ICN.
- Gender –Assists in uniquely identifying the person's record.
- Last activity date –Assists in identifying the last time the record was treated at a VA medical center.
- Date of Death –VA indicator that the person could be deceased.
- Multiple birth indicator –Yes/No field to assist with in uniquely identifying the person's record.
- Place of Birth City –Assists in uniquely identifying the person's record.
- Place of Birth State –Assists in uniquely identifying the person record.
- Mother's Maiden name –Assists in uniquely identifying the person's record.
- Claim number –Assists with person's identification.

This section contains the usage of the information highlighted in section 1.2 (MPI Primary View, MPI Correlation, MPI User Identity, IAM Application/System, IAM Provisioning).

MPI Primary View traits listed below are used to establish a VA Enterprise view of the VA identity of interest to be shared with all VA systems so that we have a single view for that identity across all VA Lines of Business (LOB) and the systems that support those VA LOB.
- Integration Control Number (ICN) –Unique VA Identification (ID) number used to bring all separate SourceIDs together across the enterprise.
- ICN status –ID status for the ICN; used to indicate whether the ICN is the current active VA ID or if it has been deactivated. Each deactivated ICN would have a corresponding active ICN.

- Name –Assists in uniquely identifying the person’s record.
- Social Security Number (SSN) –Assists in uniquely identifying the person’s record.
- Mother’s Maiden name –Assists in uniquely identifying the person’s record.
- SSN Verification Status –Provides insight to consuming applications which SSNs have been verified/validated as either correct or not.
- Pseudo SSN Reason –Used to indicate why there is not a given SSN for a given Identity record.
- Place of Birth City –Assists in uniquely identifying the person’s record.
- Place of Birth State –Assists in uniquely identifying the person record.
- Date of birth –Assists in uniquely identifying the person’s record.
- Multiple birth indicator –Yes/No field to assist with in uniquely identifying the person’s record.
- Alias –Assists in uniquely identifying the person’s record by listing an Alias Name and SSN for a particular identity.
- ID Theft Flag – Used to identify records that are compromised by identity theft and should be limited or filtered for use by any consuming applications.
- Date of Death –VA indicator that the person could be deceased.
- Address –Assists in uniquely identifying the person’s record.
- Zip code –Assists in uniquely identifying the person’s record.
- Phone number –Assists in uniquely identifying the person’s record.
- SourceID –Number used to uniquely identify a record. The fully qualified number is unique across all facilities.
- Source –Identifies the system that was the source of the data.
- Gender –Assists in uniquely identifying the person’s record.
- Last activity date –Assists in identifying the last time the record was treated at a VA medical center.
- Claim number –Assists with person’s identification.
- Email Address – Assists in uniquely identifying the person’s record.
- Race/Ethnicity - Assists in uniquely identifying the person’s record.

MPI Correlation traits listed in section 1.2 are used to provide a cached set of traits that represent the identity in the disparate system, so the centralized MPI system can manage (link, unlink, move and/or log manual resolution tasks) the relationship of each disparate/correlated identity to the VA Enterprise Identity.

MPI User Identity traits listed in section 1.2 are used to orchestration and maintain a setup of generalized user identity values across key VA systems to support the onboarding and off-Boarding of users (Employees, Contractors, Volunteers, and other VA user types) throughout their life cycle with VA.

IAM Application/System data listed in section 1.2 is used to manage how the application/system is setup to support user access and authorizations in that system/application.

IAM Provisioning data listed in section 1.2 is used to manage the users access and authorizations around systems/applications

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

SPLUNK is used to analyze the logs and identify problems. This data contains the logging of all Identity and Access Management transactions. This data is also used to report metrics. PSM component, IMDQ Toolkit, has a compare feature that allows the IMDQ team to compare ADR information collected against MPI data. The PSIM service, through a series of discovery and updates, manages persons stored in ADR. IMDQ case workers perform patient identity management quality tasks. The outcome of these efforts is greater certainty as to the identity of Veterans/patients. User provisioning has been added to approve access to VA applications that utilize SSOi and SSOe as the authentication method. There is no data produced, rather a validation of data from MPI sources and the PIV card of the requesting user, which is passed to SSOi and SSOe to then pass the authentication rights of the user to the service being requested. Authorization Data traits table is used to correlate from data that is exposed from the SSOe and SSOi interfaces from other data partners and used for the provisioning tool. Contractor Identity collects and maintains data on VA contractors that includes but not data elements previously listed. The source of the data is the IAM/MPI and is the authoritative source and system for contractor identity. The MPI system collects data from all of the VistA sites around the country. The VA stores this information collected at the AITC data center. There are no direct tools used to analyze the data for MPI. However the data is reviewed by the VistA systems end users via the VistA GOTS (Government Off-the-shelf) application

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.

No ‘new’ data elements or information is created. There is no new data produced, rather a validation of existing provided data from MPI sources and the PIV card of the requesting user, which is passed to SSOi and SSOe to then pass the authentication rights of the user to the service being requested.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Data confidentiality and integrity is ensured via administrative, technical and physical controls. Physical access to the servers is restricted to authorized personnel in a data center at a facility with 24 hour security. Network access to servers is managed through firewalls. Access via the network requires authentication for both the application and servers. Additionally, all commercial databases and applications (e.g. Oracle databases, IBM Tivoli suite, CA Product suite, etc.) conform to the mandates of FIPS 140-2 in regards to encrypting data at rest.

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

IAM requires PIV and token access, or from the customer point of view requiring appropriate Credentialling Service Provider (CSP) privileges in order to maintain the systems that have SSN and PII data. In regard to the CSP access, the only SSN or PII that a customer would be transmitted are their own.

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

IAM requires PIV and token access for application partner access and from the customer point of view requiring appropriate Credentialling Service Provider (CSP) privileges in order to maintain the systems that have SSN and PII data. Regarding the CSP access, the only SSN or PII that a customer would be transmitted are their own after the customer requests and approves.

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?

Criteria, procedures, controls, and responsibilities regarding access is documented in the User Manuals by role. Access does require manager approval and access to the system is being monitored. Access to specific identities are not being monitored currently but changes to identities are tracked, monitored, and recorded. The responsibility of assuring safeguards for the PII is shared between the business data owner and technical owner group per VA 6500 guidelines.

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

IAM components and all the data are managed by the Veteran Relationship Management (IO) IAM Information Project Team (IPT). This body has sole responsibility to analyze each business process and system connecting to PSM and MPI. The analysis defines the proper business and technical flows as well as the appropriate operations that should be implemented for that particular business process. The decision and proper implementation is then governed by the security boundaries of the service and verified manually at multiple software project milestone checkpoints (development test acceptance, Software Quality Assurance (SQA) test acceptance, and User Acceptance Testing (UAT) test acceptance). The security boundary is managed at both a coarse grain and at a fine grain level. At the coarse grain level PSM uses VAAFI and certificate-based authentication and authorization to determine and allow or disallow the consuming system to execute specific PSM operations. At a fine grain level PSM implements a configuration file that allows or disallows the consumers to perform specific specialized implementations of those operations. This same concept is carried down to the data layer for each MPI Primary View data field and is managed by fine grain controls. The data fine grain controls are identified as the MPI Primary View data rules and as identified above those rules are governed and updated by the IAM IDM sub–Information Project Team (subIPT). Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include requiring the Annual VA Rules of Behavior and Elevated Rules of Behavior training is completed for all employees, volunteers, and contractors prior to access to the system. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. IAM has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information. All IAM administrators must have VA elevated privileged accounts. No CSP or VAEC personnel have access to IAM data, including PII.

2.4c Does access require manager approval?

Criteria, procedures, controls, and responsibilities regarding access is documented in the User Manuals by role. Access does require manager approval and access to the system is being monitored. Access to specific identities are not being monitored currently but changes to identities are tracked, monitored, and recorded. The responsibility of assuring safeguards for the PII is shared between the business data owner and technical owner group per VA 6500 guidelines.

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

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include requiring the Annual VA Rules of Behavior and Elevated Rules of Behavior training is completed for all employees, volunteers, and contractors prior to access to the system. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. IAM has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information. All IAM administrators must have VA elevated privileged accounts. No CSP or VAEC personnel have access to IAM data, including PII.

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

As for the use of the data once it leaves MPI and is pulled either into the consuming systems business process flow or into their system that is also governed by the IAM IPT. The rules of behavior are defined in several documents related and associated with each consumer's Service Request (SR). Each integration should have a BRD (Business Requirements Document), iRSD (Integration Requirements Document) and SDD (System Design Document). As identified above, the use of the PSM and MPI data is then tested via 3 quality development milestones (Development testing acceptance, SQA testing acceptance and UAT testing acceptance) and once those are signed off then the consumer can go into production.Each release and integration go through the quality milestone gates described above and within each of those is some form of training and knowledge transfer relative to the data, process, functionality and capability of the system and service.

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*

MPI Primary View only contains a minimal set of data traits that is gathered from the key VA Line of Business (LOB) systems that capture the identity information of persons of interest to VA. Once the data is captured it is related indefinitely to support MPI mission and scope as the Authoritative data source/service for all identity persons of interest to VA.

MPI Correlation contains the minimal data needed to perform basic matching as well as secondary manual matching activities to support the matching of these disparate system identities and identifiers to the Enterprise Identity. Once the data is captured it is retained indefinitely and is kept in sync and audited.

MPI User Identity contains the minimal data traits gathered from key user stores across all VA systems and this data is used to map all VA users to a single Enterprise Identity for sharing of that key user information across key user data stores (AD, TMS, IAM PROVISIONING, IAM SSOi/SSOe) to reduce manual data entry and therefore data quality differences across those key systems. This data is only temporarily stored as part of the user onboarding process and is not retained beyond that onboarding life cycle process. If the data is needed beyond that lifecycle it is pulled/obtained from the authoritative sources.

PII on the information system is also captured during the audit data collected in the process of completing transactions and authentications to the system. Name, Social Security, Date of Birth, Mailing address Zip code, email, phone number, UserID, eAL1, eAL2, eAL3, eAL4 (Electronic Authentication Assurance Level), Authentication Tokens; password, PIN, Public Key Infrastructure (PKI) on Smart Card, Soft Certificate will be retained as part of the audit record and will be used for audit purposes only.

MPI data retained
Integration Control Number (ICN), Surname, First Name, Middle Name, Name Prefix, Name Suffix, Mother's Maiden Name, Date of Birth, Place of Birth City (POBC), Place of Birth State (POBS), Date of Death, Death Verification Status, Gender, Social Security Number (SSN), SSN Verification Status, Pseudo SSN Reason, Coordinating Master of Record, Sensitivity, Primary ICN, Date/Time of Original Creation, Facility of Original Creation, Created By, Resolution Journal Case Number, Primary View Date Last Updated, Identity Theft, Temporary ID Number, Foreign ID Number, Street Address [Line 1], Street Address [Line 2], Street Address [Line 3], City [Residence], State [Residence], Zip+4 [Residence], Phone Number [Residence], Multiple Birth Indicator, Province Postal Code, Country, Alias, Alias Surname, Alias First Name, Alias Middle Name, Alias Prefix, Alias Suffix, Alias SSN, Alias Date Last Updated, Race Information, Race Date Last Updated, Ethnicity Information, Ethnicity Date Last Updated, ID State, Date of ID State, Surname Primary View Score, First Name Primary View Score, Middle Name Primary View Score, Prefix Primary View Score, Suffix Primary View Score, DOB Primary View Score, Gender Primary View Score, SSN Primary View Score, MMN Primary View Score, Mult Birth Primary View Score, POB City Primary View Score, POB State Primary View Score.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

IAM-E/AcS data is retained per NARA GRS 3.2, item Information System Security Records to provide historical reports and to be available as needed for investigations or other legal reasons. GRS

3.2, item 031. Covers User Identification, Profiles, Authorizations, and Password Files and at time of publication requires a 6-year retention period from time of user account termination. System logs are retained for one year unless needed for audit or investigation.For PSM, All MPI Primary View and Correlation data current and past audit information is retained and without any currently defined purging requirements. Also, all identity resolution and associated resolution audit information is retained with no currently defined purging requirements. The only data that is purged is the specific transactional data coming in and going out through the interfaces. That data is purged specific to the disk availability allows at any given time (currently purged at 6 months to one year).MPI Primary View data once captured is related indefinitely to support MPI mission and scope as the Authoritative data source/service for all identity persons of interest to VA.MPI Correlation data once captured is retained indefinitely and is kept in sync and audited.MPI User Identity data is only temporarily stored as part of the user onboarding process and is not retained beyond that onboarding life cycle process. If the data is needed beyond that lifecycle it is pulled/obtained from the authoritative sources.IAM Application/System contains data about an application/system to support the onboarding/off-boarding of user access to those systems. Once this data is captured it is retained indefinitely.IAM Provisioning contains data about the provisioning of a user to a system. This data once captured is retained indefinitely.For MPI, all data current and past audit information is retained and without any currently defined purging requirements. The only data that is purged is the specific transactional data coming in and going out through the interfaces. That data is purged specific to the disk availability allows at any given time (currently purged at 75 years).

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

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

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

The retention schedule been approved by the National Archives and Records Administration (NARA), NARA GRS 3.2, Information System Security Records to provide historical reports and to be available as needed for investigations or other legal reasons. GRS 3.2, item 031. covers User Identification, Profiles, Authorizations, and Password Files and at time of publication requires a 6yr retention period from time of user account termination. System logs are retained for one year unless needed for audit or investigation. https://www.archives.gov/files/records-mgmt/grs/grs03-2.pdf

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

Per the Department of Veterans Affairs Records Control Schedule 10-1, 6000.2 Electronic Health Record[s] (EHR) are to be retained 75 years after last episode of patient care (N1-15-02-

3, Item 3). Electronic Records were superseded by General Records Schedule 4.3 (item 40); however, per the National Archives General Records Schedules Crosswalk, the new General Records Schedule is 5.2 020. GRS 5.2 Intermediary Records disposition allows for disposal when no longer needed for business use.Per the Patient Medical Records-VA (24VA10A7) System of Record, records and information are maintained electronically for seventy-five years after the last episode of patient care and then deleted. Per the National Patient Databases-VA (121VA10A7) System of Record, disposal is in accordance with General Records Schedule 20, item 4. Item 4 provides for deletion of data files when the agency determines that files are no longer needed for administrative, legal, audit or other operational purposes. Per the National Archives General Records Schedules Crosswalk, the new General Records Schedule is 5.2 020. GRS 5.2 Intermediary records disposition allows for disposal when no longer needed for business use.MPI's disposal procedure can be found in Deferral Register Volume 66, No. 133. Records are maintained and disposed of in accordance with record disposition authority approved by NARA.

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.

Once records are entered into the system they remain as part of the protected system information. System logs are maintained for one year and then flagged for deletion by their automated processes. System logs are not retained after one year and any SPI containing them will be overwritten as part of the process for audit management. When virtual machines are no longer required to support the system, they are wiped clean and the data overwritten.Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2.In addition, any equipment that is decommissioned and is leaving the controlled data center will be sanitized (e.g., degaussing) or destroyed in accordance with VA Handbook 6500 and the Veterans Affairs Dedicated Cloud Media Sanitization Procedure. VA Dedicated Cloud Media Sanitization policy outlines the VA Dedicated Cloud policy and procedure for tracking, documentation and disposal of storage media within the environment and their return to the VA, in accordance with VA Handbook 6500.For MPI, depending on the record medium, records are destroyed by either shredding or degaussing. Optical disks or other electronic media are deleted when no longer required for official duties. Archived records are labeled with a disposal date beyond which they can be shredded. Retention of electronic records is the responsibility of the MPI's System Manager.Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization

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.

PII is not used for research, testing or training in IAM.

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

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

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

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

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

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

Follow the format below:

<u>Privacy Risk:</u> There is a risk to maintaining data within the IAM system is that longer retention times increase the risk that information can be compromised or breached.
MPI records are to be maintained for a minimum of seventy-five years after the death of the veteran or after date of last contact in the event of medical or legal review. There are currently no purge requirements defined for MPI.

PSM records are to be maintained for a minimum of seventy-five years after the death of the veteran or after date of last contact in the event of medical or legal review. There are currently no purge requirements defined for PSM.

<u>Mitigation:</u> IAM follows NARA approved GRS 3.2 Information System Security Records to provide historical reports and to be available as needed for investigations or other legal reasons GRS 3.2, item 031 covers User Identification, Profiles, Authorizations, and Password Files and at time of publication requires a 6 year retention period from time of user account termination. System logs are retained for one year unless needed for audit or investigation. When the retention data is reached for a record, the IAM team will carefully disposes of the data. All electronic storage media used to store, process, or access VA Sensitive Information including PII will be disposed of in adherence with the latest version of VA Handbook 6500.1, Electronic Media Sanitization.

MPI mitigates this risk by maintaining audit data such as Date Last Updated as well as linking and capturing the data from other internal VA systems including Person Service Identity Management (PSIM), Identity Management Toolkit (IdM TK) and VistA sites to try and keep it as accurate as possible.

PSM mitigates this risk by maintaining audit data such as Date Last Updated as well as linking and capturing the data from many different internal VA sources as well as DoD DEERS to try and keep it as accurate as possible. Future mitigation strategies are also being put into place to obtain data from a 3rd party vendor system tied to credit reports to get updates outside of VA and DoD.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Single Sign-on enabled applications	To authenticate Veterans to VA Information systems using a single login credentials from outside VA	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Lightweight Directory Access Protocol over Secure Socket Layer (SSL) (LDAPS) and Security Assertion Markup Language (SAML)
VA credential service provider (VA Logon)	To authenticate Veterans to VA Information systems using a single login credentials from outside VA	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	SAML
VA MPI	To authenticate Veterans to VA Information systems	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Simple Object Access Protocol (SOAP) over HTTPS using SSL encryption and Certificate exchange
MPI	In conjunction with PSM, MPI is the authority to the VA on person identity.	MPI Primary View data traits with ICN (ICN, ICN Status, Name, SSN, Mother's Maiden Name, SSN Verif Status, Pseudo SSN Reason, Place of Birth City, Place of Birth State, Date of Birth, Multiple Birth Indicator, Alias, ID Theft Flag, Date of Death, Address and Phone Number) MPI Correlated IDs (ID, IDType, Assigning Authority, Assigning Facility and SourceID state)	VistALink Remote Procedure Call (RPC) Transmission Control Protocol (TCP)/Minimum Lower Layer Protocol (MLLP)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
ADR	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Java Database Connectivity (JDBC)
ESR	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Enterprise JavaBeans (EJB) Webservice
HDR CDS	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Hyper Text Transfer Protocol Secure (HTTPS)
VAAFI for consuming applications	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Automated communications over Hyper Text Transfer Protocol Secure (HTTPS)
BizFlow	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address MPI Correlated IDs	Via IAM DataPower
CAPRI	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence	Via IAM DataPower

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		Address, Home Phone, Correspondence Address	
CRS	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Via IAM DataPower
EBN	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Via IAM DataPower
FSC	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Via IAM DataPower
HAPE	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Via IAM DataPower
HRA	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Via IAM DataPower
HRC	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of	Via IAM DataPower

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	
JLV	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Via IAM DataPower
NHIN	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Via IAM DataPower
North Chicago Common Registration UI	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Via IAM DataPower
NVP (VAP) CPP	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Via IAM DataPower
SSOe	Person identification	May include: Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone, Correspondence Address	Via IAM DataPower

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
PSIM	PSIM is part of the overall MPI architecture so the MPI data is replicated into the ADR/PSM schema to support our SOAP and RestFul client interfaces	Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone	MLLP SOAP/XML RPC
Veterans Information Systems and Technology Architecture (VistA)	MPI is the authoritative source for all VA persons of interest in the VA and as such MPI receives and pushes the authoritative Identity Information to VistA to store and use to support it's business purpose	Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone	MLLP RPC
HomeTelehealth	HomeTelehealth implemented the Decentralized Hybrid Integration pattern with MPI and as such received Telehealth information form VistA and corresponds with MPI to	Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone	MLLP

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
	obtain the latest identity data on those patients receiving telehealth support		
Blind Rehabilitation BLIND REHAB SYSTEM (AUSTIN)	Blind Rehab implemented the Decentralized Hybrid Integration pattern with MPI and as such received Telehealth information form VistA and corresponds with MPI to obtain the latest identity data on those patients receiving telehealth support	Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone	MLLP
MyHealtheVet	MHV implemented the Enterprise Integration pattern with MPI and as such receives identity updates for their MHV user population from MPI	Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN, Correspondence Address, Home Phone	MLLP & Datapower
Corporate Data Warehouse (CDW)	CDW utilizes the identity data received from MPI for their VA	Name, DOB, SSN, Mothers' Maiden Name, Place Of Birth, Gender, Date Of Birth, Date Of Death, Multiple Birth Indicator, Alias Name and SSN,	Cache Shadow

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
	Enterprise Analytics and Reporting purposes	Correspondence Address, Home Phone	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk:
1)There is a risk that information may be shared with unauthorized VA programs or systems.

2)The MLLP protocol the VistA uses to communicate with the MPI transmits PII data without encryption.

3)As the VA brings up more and more systems in the future, more applications will be querying PSM to retrieve and/or verify identities.

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

2)Plans are to address this as well as system authentication requirements in future enhancements to the interface. No firm date has been announced for these enhancements. The protocol itself does not support encryption, but encryption can be added through TLS.

3)The IAM Information Project Team (IPT) manages PSM and its data. This body has sole responsibility to analyze each business process and system connecting to the software. The analysis defines the proper business and technical flows as well as the appropriate operations that should be implemented for that particular business process. The decision and proper implementation is then governed by the security boundaries of the service and verified manually at multiple project milestone checkpoints.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

shared/received with	***transmitted with the specified program office or IT system***		***routine use, etc. that permit external sharing (can be more than one)***	***place to secure data***
Data Center (DMDC), DoD	The information is used to authenticate a user to an application	Names, Social Security Number, Phone Numbers, **May include: Name, DOB, Mothers' Maiden Name, PlaceOfBirth, Gender, DateOfBirth, DateOfDeath, , Alias Name and Correspondence Address, Home Phone, Correspondence Address*	Defense Civilian Personnel Data System DPR34, 138VA005Q DOD/VA MOU	Encrypted data communication pathways
U.S. Coast Guard	The information is used to authenticate a user to an application verifying their identity.	Names, Social Security Number, Phone Number, date of birth, UserID, eAL1, eAL2, eAL3, eAL4 (Electronic Authentication Assurance Level) Authentication Tokens; password, PIN, phone number, PKI on Smart Card, Soft Certificate	DPR34, 138VA005Q	Encrypted data communication pathways
Public Health Service	The information is used to authenticate a user to an application verifying their identity.	Names, Social Security Number, Phone Number, date of birth, UserID, eAL1, eAL2, eAL3, eAL4 (Electronic Authentication Assurance Level) Authentication Tokens; password, PIN, phone number, PKI on Smart Card, Soft Certificate	DPR34, 138VA005Q	Encrypted data communication pathways
DS Logon	The information is used to authenticate a user to an application verifying their identity.	Names, Social Security Number, Phone Number, date of birth, UserID, eAL1, eAL2, eAL3, eAL4 (Electronic Authentication Assurance Level) Authentication Tokens; password, DPR34, 138VA005Q Encrypted data communication pathways PIN, phone number, PKI on Smart Card, Soft Certificate	DPR34, 138VA005Q	Encrypted data communication pathways

Veterans and Dependents Human Resource Information System (HRIS) Share Service Center (SSC))”	The information is used to authenticate a user to an application verifying their identity.	Names, Social Security Number, Phone Number, date of birth, UserID, eAL1, eAL2, eAL3, eAL4 (Electronic Authentication Assurance Level) Authentication Tokens; password, DPR34, 138VA005Q Encrypted data communication pathways PIN, phone number, PKI on Smart Card, Soft Certificate	DPR34, 138VA005Q	Encrypted data communication pathways
Government Printing Office Veterans Health Identification Card (VHIC)	Printing of Veteran Health Card	Names, Social Security Number, Phone Number, date of birth, UserID, eAL1, eAL2, eAL3, eAL4 (Electronic Authentication Assurance Level) Authentication Tokens; password, DPR34, 138VA005Q Encrypted data communication pathways PIN, phone number, PKI on Smart Card, Soft Certificate Benefits	DPR34, 138VA005Q	Encrypted data communication pathways
Login.gov	Login.gov -- The information is used to authenticate a user to an application verifying their identity.	Names, Social Security Number, Phone Number, date of birth, UserID, eAL1, eAL2, eAL3, eAL4 (Electronic Authentication Assurance Level) Authentication Tokens; password, DPR34, 138VA005Q Encrypted data communication pathways PIN, phone number, PKI on Smart Card, Soft Certificate	IAM-Login.gov MOU	Encrypted data communication pathways
ID.me	ID.me -- The information is used to authenticate a user to an application verifying their identity.	Names, Social Security Number, Phone Number, date of birth, UserID, eAL1, eAL2, eAL3, eAL4 (Electronic Authentication Assurance Level) Authentication Tokens; password, DPR34, 138VA005Q Encrypted data communication pathways PIN, phone number, PKI on Smart Card, Soft Certificate	IAM-ID.me MOU	Encrypted data communication pathways

DoD DEERS	Department of Defense - Defense Enrollment Eligibility Reporting System	Names, Social Security Number, Phone Numbers, **May include: Name, DOB, Mothers' Maiden Name, PlaceOfBirth, Gender, DateOfBirth, DateOfDeath, , Alias Name and Correspondence Address, Home Phone, Correspondence Address*	National MOU	Encrypted data communication pathways Via IAM VAAFI

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

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

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with an external organization or agency that does not have a need or legal authority to access VA data.

Mitigation: Safeguards are implemented to ensure data is not shared with unauthorized organizations, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized for the system. Interconnection Security Agreements (ISA) and Memoranda of Understanding (MOU) are kept current and monitored closely to ensure protection of information.

Section 6. Notice

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

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

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:1. The System of record Notice (SORN) “National Patient Databases-VA” 121VA10A7. The SORN can be found online at: http://www.gpo.gov/fdsyesys/pkg/FR-2004-04-07/pdf/04-7821.pdf. Further, SORNs 24VA10A7, 150VA19 and 138VA005Q apply.2. This Privacy Impact Assessment (PIA) also serves as notice of the PITC Insurance Paymentsystem. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), theDepartment of Veterans Affairs “after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.”A notification banner with notification of users of how the information will be collected: “VA information resides on and transmits through computer systems and networks funded by VA”And the purposes of collection:” This system is intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized”PII is collected in order to provide services to the Veteran community. The Veteran has the ability to opt out of the process. The form VA Form 10-10EZ, Application for Health Benefits, collects PII in order to provide health benefits to Veterans. The form states why the information is being collected “VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705, 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.”The VHIC, a component of IAM, is issued only to Veterans who are enrolled in the VA health care system. VA Form 10-10EZ, Application for Health Benefits, provides the following Privacy Act information:VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705, 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified from initial submission forward through a computer-matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the VHA Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social

Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.In addition, there are cancel and continue buttons that a user can opt to continue or cancel if they do not want to provide information to continue

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

A notification banner with notification of users of how the information will be collected: “VA information resides on and transmits through computer systems and networks funded by VA”And the purposes of collection:” This system is intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized”PII is collected in order to provide services to the Veteran community. The Veteran has the ability to opt out of the process. The form VA Form 10-10EZ, Application for Health Benefits, collects PII in order to provide health benefits to Veterans. The form states why the information is being collected “VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705, 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.”
6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

A notification banner with notification of users of how the information will be collected: “VA information resides on and transmits through computer systems and networks funded by VA”And the purposes of collection:” This system is intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized”PII is collected in order to provide services to the Veteran community. The Veteran has the ability to opt out of the process. The form VA Form 10-10EZ, Application for Health Benefits, collects PII in order to provide health benefits to Veterans. The form states why the information is being collected “VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705, 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.”The VHIC, a component of IAM, is issued only to Veterans who are enrolled in the VA health care system. VA Form 10-10EZ, Application for Health Benefits, provides the following Privacy Act information:VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705, 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified from initial submission forward through a computer-matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the VHA Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.In addition, there are cancel and continue buttons that a user can opt to continue or cancel if they do not want to provide information to continue

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.

Users are told specifically in “VA Form 10-10EZ Application for Health Benefits” that providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of their request for health care benefits. Veterans are also informed that “failure to furnish the information will not have any effect on any other benefits to which you may be entitled.”

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.

A notification banner with notification of users of how the information will be collected: “VA information resides on and transmits through computer systems and networks funded by VA”And the purposes of collection:” This system is intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized”PII is collected in order to provide services to the Veteran community. The Veteran has the ability to opt out of the process. The form VA Form 10-10EZ, Application for Health Benefits, collects PII in order to provide health benefits to Veterans. The form states why the information is being collected “VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705, 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law. Data stored by the MPI is received from VistA and CPE. The MPI does not collect any information directly from veterans or their dependents. PSM does not directly collect data from people; therefore, there is no possibility of information denial. All data for PSM comes from other systems.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

<u>Privacy Risk:</u>
There is a risk that VA employees will not know that IAM collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

<u>Mitigation:</u>
The IAM mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the methods discussed in question 6.1. This system is maintained under the legal authority of Title 38, USC, Section 501 and Section 7304.
The Privacy Act permits VA to disclose information about individuals without their consent for a routine use when the information will be used for a purpose that is compatible with the purpose for which VA collected the information. The SORNs, DPR 34, 138VA005Q, and 24VA10A7 permits sharing information with DMDC (a DoD organization) and other external applications. Information is only used to for the purpose it was collected and this system is maintained under the legal authority of Title 38, USC, Section 501 and Section 7304 Privacy Act System of Records Notice 138VA005Q, (Supplementary Information paragraph b, section 2) dated 7/27/2009. https://www.oprm.va.gov/privacy/systems_of_records.aspx
The Master Person Index (MPI) System of Records Notice (SORN) 24VA10A7 is found at the following link: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

The SORN also provides individuals who wish to determine whether a record is being maintained in this
system under his or her name or other personal identifier, or wants to determine the contents of such record can contact the VA facility location at which they are or were employed or treated or

made or have contact. However, as noted above, provision of all requested information is a requirement for VA benefits.

Section 7. Access, Redress, and Correction

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

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

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

*7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions**. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

IAM provides federated identity services that allow veterans or authorized persons of interest to establish a single authenticated identity through a trusted provider (either external or internal to VA), which they can use to access internal VA applications as well applications of other participating government agencies. No user can gain access to the system without authentication to the system through a CSP.A user must log in through a Credential Service Provider (CSP) using a user id and password. Some CSPs require two factor authentications to verify the identity. There is no method on IAM systems for users to gain access to their information except employees and contractors to VA systems can update their own information. No External users to IAM systems can make changes to their identity information except for the VHIC application. Users are prompted to confirm information at the time of card issue.

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).

IAM is not exempt from any provisions of the Privacy Act.

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.

Individuals wishing to obtain more information about access, redress and record correction of the Master Patient Index, should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) "National Patient Databases-VA" 121VA10A7 (April 7, 2004).

This SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdfAn individual will not gain access to their information in PSM. They can access their data through other systems such as MPI, ESR, ADR and HDR CDS and those systems can update the record in PSM.

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.

Veterans Health Administration (VHA) Directive 2012-036, Identity Authentication for Health Care Services, provides policy and procedures to authenticate the identity of individuals requesting VA medical care, treatment, or services in person and provides administrative correction procedures to correct information previously captured by, or in, error. AUTHORITY: Privacy Act of 1974, Title 5 United States Code (U.S.C.) 552a, Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, Title 45 Code of Federal Regulations (CFR) Part 160 and 164.The VA website provide numerous avenues that notify individuals of the procedures for updating their information. Individuals seeking to make changes to their records may use VA Form 10-10EZR, Instructions for Completing Health Benefits Update Form. Individuals may also interface with VA Patient Advocates for guidance at facilities where the Veterans Identification Cards are issued. Individuals are also prompted to confirm information at time of VHIC application on the VA VHIC application website. The VA, Veterans Service Organizations, and other Veteran advocate organizations also support the education of and notification process for Veterans.Individuals wishing to obtain more information about access, redress and record correction of the Master Patient Index, should contact the Department of Veteran’s Affairs regional as directed in the System of Record Notice (SORN) “National Patient Databases-VA” 121VA10A7 (April 7, 2004). This SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf

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.

IAM systems do not input any data from Veterans except what is captured to obtain a Veteran Health Benefit Card. The information provided to obtain and secure a VHIC card must already be captured in a system or Database external to IAM control. Veteran information must already be captured in the MPI system or in a Credential Service Provider. Veterans must complete VA Form 10-10EZR, Instructions for Completing Health Benefits Update Form which is outside the scope and control of IAM. Individuals may also interface with VA Patient Advocates for guidance at facilities where the Veterans Identification Cards are issued. Individuals are also prompted to confirm information at time of VHIC application on the VA VHIC application website. The VA, Veterans Service

Organizations, and other Veteran advocate organizations also support the education of and notification process for Veterans.Individuals wishing to obtain more information about access, redress and record correction of the Master Patient Index, should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) "National Patient Databases-VA" 121VA10A7 (April 7, 2004). This SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdfUnder the jurisdiction of VHA, VHA Directive 1605.1 establishes the VHA privacy practices procedures for the use and disclosure of individually-identifiable information, and individual privacy rights related to VHA health care data, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

Credential Service Provider change information cannot be made on the IAM application. There is no mechanism to input or change credential or user data on the system. That information is provided externally by VA CPS and Third party CSPs.VA website provide numerous avenues that notify individuals of the procedures for updating their information which are external to VA IAM control or responsibility except that information used to generate VHIC. IAM used data already verified internally or externally. Individuals seeking to make changes to their records may use VA Form 10-10EZR, Instructions for Completing Health Benefits Update Form. Individuals may also interface with VA Patient Advocates for guidance at facilities where the Veterans Identification Cards are issued. Individuals are also prompted to confirm information at time of VHIC application on the VA VHIC application website. The VA, Veterans Service Organizations, and other Veteran advocate organizations also support the education of and notification process for Veterans. IAM administrators have no ability to view or modify user data. Individuals wishing to obtain more information about access, redress and record correction of the Master Patient Index, should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) "National Patient Databases-VA" 121VA19 (April 7, 2004). This SORN can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2004-04-07/pdf/04-7821.pdf Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information, section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk:
1)There is a risk that individuals whose records contain incorrect information may not receive notification on how to redress or correct their information.

2)There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

3)There is a risk that individuals whose records contain incorrect information may not receive notification on how to redress or correct their information.

4)There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation:

1)IAM systems do not input any data from Veterans except what is captured to obtain a Veteran Health Benefit Card. The information provided to obtain and secure a VHIC card must already be captured in a system or Database external to IAM control. Veteran information must already be captured in the MPI system or in a Credential Service Provider.
VA website provide numerous avenues that notify individuals of the procedures for updating their information which are external to VA IAM control or responsibility except that information used to generate VHIC. IAM used data already verified internally or externally. Individuals seeking to make changes to their records may use VA Form 10-10EZR, Instructions for Completing Health Benefits Update Form.
Individuals may also interface with VA Patient Advocates for guidance at facilities where the Veterans Identification Cards are issued. Individuals are also prompted to confirm information at time of VHIC application on the VA VHIC application website. The VA, Veterans Service Organizations, and other Veteran advocate organizations also support the education of and notification process for Veterans. IAM administrators have no ability to view or modify user data for veterans or other users to IAM systems.

2)By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

3) IAM systems do not input any data from Veterans except what is captured to obtain a Veteran Health Benefit Card. The information provided to obtain and secure a VHIC card must already be captured in a system or Database external to IAM control. Veteran information must already be captured in the MPI system or in a Credential Service Provider.

4) By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

Section 8. Technical Access and Security

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

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

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

In accordance with the SORN noted above in Section 6.2 and national and locally established data security procedures, access to access services information databases (HEC Legacy system and the Enrollment Database) is controlled by unique entry codes (access and verification codes). The user's verification code is automatically set to be changed every 90 days. User access to data is controlled by role-based access as determined necessary by supervisory and information security staff as well as by management of option menus available to the employee. Determination of such access is based upon the role or position of the employee and functionality necessary to perform the employee's assigned duties.On an annual basis, employees are required to sign a computer access agreement acknowledging their understanding of confidentiality requirements. In addition, all employees receive annual privacy awareness and information security training. Access to electronic records is deactivated when no longer required for official duties. Recurring monitors are in place to ensure compliance with nationally and locally established security measures.(OI&T) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance: along with formal, documented procedures to facilitate the implementation of the control policy and associated controls. OI&T documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed the Talent Management System (TMS).

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

No users from other agencies can log into IAM systems or assets. SSOi and SSOe allow other agencies/partners to authenticate users to their systems. These other systems are where users would log in. Other systems, such as Vista and may have connections to MDM. VHIC is the only system where users log in to view basic information. That is a finite set of users for creating customer cards but cannot access information within IAM

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.

There are no typical users within IAM and hence no 'roles' for describing different levels of user access. No 'users' to change, alter, append, delete or add information within IAM. All data is on other systems and IAM provides provisioning to support SSOi and SSOe.

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

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

The target user population for IAM is any system user accessing a secured VA application available on the public Internet, potentially the entire Veteran population, their dependents, VA's customers and business partners including but not limited to contractors and other users to the information system. Contractors are required to complete the same provisioning, onboarding and training requirements as all VA users prior to access to VA Information Systems including IAM-E. VA COR review and manage contracts and non-disclosure agreements approved by VA. The COR oversees the contracts awarded to contract personnel. No Contractor access to information system is granted without VA COR approval. No contractor, volunteer, or employee has any access to VA information systems and PII until they have been fully on boarded. Only IAM SA with VA elevated Privilege accounts have access to the IAM system and Contractors as well as VA employees receive annual training regarding their roles on the system and sign a "Rules of Behavior for EP" that prevents VA contractors from using PII in any manner not consistent with business needs. IAM ensures screening is conducted for all contract personnel and federal employees and all other appointed workforce members. The onboarding process consists of screening, as defined by VA Directive and Handbook 0710 Personnel Suitability and Security Program, of federal employees and contract personnel who participate in the design, development, operation, or maintenance of sensitive applications and sensitive systems, as well as those individuals having access to VA sensitive information or information is required.

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.

VA and IAM provide security and privacy awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by information system changes, and annually thereafter

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 7/1/2022
3. *The Authorization Status: ATO Granted*
4. *The Authorization Date:* 7/22/021
5. *The Authorization Termination Date:* 7/21/2024
6. *The Risk Review Completion Date:* 7/1/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* 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.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes; IAM and all sub-systems are in the VAEC Microsoft Azure Government (MAG) environment. The VAEC MAG is FedRAMP approved by the VA

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

VAEC

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.

VAEC

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.

VAEC

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).

VAEC

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

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

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.05.31 15:39:07 -04'00'

Privacy Officer, Tonya Facemire

Digitally signed by WADE STROMER
Date: 2023.05.31 13:45:33 -06'00'

Information System Security Officer, Wade Stromer

KEVIN J. WILLIS 476920

Digitally signed by KEVIN J. WILLIS 476920
Date: 2023.06.01 08:11:32 -04'00'

Information System Owner, Kevin Willis

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).

This system is maintained under the legal authority of Title 38, USC, Section 501 and Section 7304. Identity and Access Management is not a System of Records and the only PII received from the system is data from Master Veterans Index (MPI) which is a System of Record. The MPI System of Record Notice is 24VA10A7 Patient Medical Records-VA and also System of Records 121VA10A7 – National Patient Databases-VA.
https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf

The SORN, 24VA10A7 - Patient Medical Records-VA permits IAM-E correlation of data, to include PII, with the Master Veterans Index (MPI). Additionally, VA internal consuming applications may request specific data from IAM-E services that may include PII.
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

Related to the Privacy Act, SORN 150VA19 (2022) - Administrative Data Repository-VA states the records in this system include identifying information including Social Security Number, contact information, educational background, financial information, military service and eligibility information for VHA patients and their providers.
https://www.govinfo.gov/content/pkg/FR-2008-11-26/pdf/E8-28183.pdf

SSO-e or VAAFI, a component of Identity Access Management does not collect the information on behalf of its users. The system checks accuracy against the stored credentials to provide access to VA/ DOD applications. User’s information and PII accessed by VAAFI comes from Credential Service Providers external to the system.

There are multiple MOUs for the external Credential Service Providers, and they are listed in the table below. The Privacy Act permits VA to disclose information about individuals without their consent for a routine use when the information will be used for a purpose that is compatible with the purpose for which VA collected the information.

VA 138VA005Q, Veterans Affairs/Department of Defense Identity Repository (VADIR)-VA”

(Supplementary Information paragraph b, section 2) dated 7/27/2009 permits the collection of information for the application and verification of military benefits for Veterans. DPR 34 allows the collection of PII for the purposes of establishing human resources records. E9-17776.pdf (govinfo.gov) and https://www.oprm.va.gov/privacy/systems_of_records.aspx http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Article-View/Article/570697/dpr-34- dod/

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices