Privacy Impact Assessment for the VA IT System called:

Summit Data Platform

Data and Analytics

Veterans Affairs Corporate Office (VACO)

eMASS ID #1301

Date PIA submitted for review:

10/10/2023

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)	Albert Estacio	Albert.Estacio@va.gov	909-583- 6309
Information System Owner	Manvendra Jhala	Manvendra.jhala@va.gov	512-981-4929

Abstract

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

The Summit Data Platform (SDP) is an open-architected, multi-cloud data enterprise data management and analytics platform. SDP delivers an integrated suite of tools for the ingestion, conditioning, and curation of multi-source data sets into consumable data products. The platform is open to data scientists, analysts and product teams that require end-to-end solutions for the creation of enterprise data products. SDP provides the VA with an Enterprise data lake and facilitates the interoperability of key data platforms to ensure consistent and secure access to data regardless of its system of origin or curation. The platform enables evidence-based decision making to improve outcomes for Veterans and their families through the delivery of data insights to VA employees across Administrations.

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?
Summit Data Platform - Data and Analytics

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
The Summit Data Platform (SDP) is the VA's quintessential source for all veteran experience and health data. SDP is a core component of business intelligence that provides historical, real-time, and predictive views of enterprise operations enabling evidence-based decision making to improve outcomes for Veterans and their families through the delivery of data insights to VA employees across Administrations.

C. Who is the owner or control of the IT system or project?
VA Owned and VA Operated

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?
SDP audience is currently estimated at 2065 users.

E. What is a general description of the information in the IT system and the purpose for collecting this information?
SDP aggregates veteran data obtained from various disparate data sources across VA. These data sources include but are not limited to: Telephone Carriers, Interactive Voice Response (IVR), Automatic Call Distributors (ACD), Customer Relationship Management (CRM), White House Hotline, Survey Data, Virtual Chatbot Transcripts, Corporate Data Warehouse, Palantir and so on.

SDP provides an opportunity to:
•Integrate veteran data from multiple sources into a single database and data model
•Maintain veteran experience history and health data
•Integrate data from multiple source systems, enabling a central view across the enterprise
•Improve data quality and present the organization's information consistently
•Provide a single common data model for all data of interest regardless of the data's source
•Restructure the data to make better decisions
•Deliver enhanced business intelligence
•Perform predictive analysis for medical trends across clinics, patients, or contact center information
•Proactive reach out to veterans based on predictive patterns
•Develop predictive Key Performance Indicator (KPI) reporting for better performance and outcome
•Improve workforce management recommendations based on medical trends across clinics, patients, or contact center inform

F. 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?

SDP aggregates veteran data obtained from various disparate data sources across VA. These data sources include but are not limited to: Telephone Carriers, Interactive Voice Response (IVR), Automatic Call Distributors (ACD), Customer Relationship Management (CRM), White House Hotline, Survey Data, Virtual Chatbot Transcripts, Corporate Data Warehouse, Palantir and so on.

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

No

3. Legal Authority and SORN

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

The current System of Records Notice (SORN) are applicable, but some will need to be updated or modified for this system or collection. The applicable legal authority falls under SORN: 23VA10NB3: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111,501, 1151 1703, 1705, 1710, 1712, 1717,1720, 1721, 1724, 1725, 1727, 1728,1741 – 1743, 1781, 1786, 1787, 3102,5701 (b) (6) (g) (2) (g) (4) (c) (1), 5724, 7105,7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014 and SORN 54VA10NB3: Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101. Additional SORNs are 158VA10NC5, 172VA10/ 86 FR 72688, 24VA10A7, 173VA005OP2, 58VA21/22/28, 197VA10, 48VA40B, 42VA41, 100VA10H, 155VA10NB / 88 FR 63678, 27VA047/ 77 FR 39346, 45VA21/ 88 FR 7776, 65VA122/74 FR 33024, 75VA001B/ 87 FR 36584, 79VA10 / 85 FR 84114, 89VA10NB/ 78 FR 76897, 90VA194/ 74 FR 17283, 113VA112/ 74 FR 21742, 114VA10/ 86 FR 6996, 130VA10P2/ 81 FR 58005, 147VA10/ 86 FR 46090, 168VA005/ 86 FR 6975, and 180VA10D/ 86 FR 46097.

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.

4. System Changes

J. *Will the completion of this PIA will result in circumstances that require changes to business processes?*
No

K. *Will the completion of this PIA could potentially result in technology changes?*
No

Section 1. Characterization of the Information

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers

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

☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒ Gender
☒ Integrated Control Number (ICN)
☒ Military History/Service Connection
☒ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Activity tracker data, Admit Date Time, Age, Age range, Applicant Type, Benefits End Date, Benefits Information, Biometrics, bothering symptoms, bothering symptoms Label, Call Center, Caregiver ID, Caregiver Integration Control Number (ICN), Caregiver Status, Case updates, City of residence, Claims Decision, complaints, compliments, Consult, Contact History, contact information, County of residence, Covid 19 (U09_9) Date Assigned, COVID case information, Covid ICD10 Codes (international classification of diseases version 10), Customer Name, Customer VBA-generated documentation, Customer VHA-generated documentation, Dashboard Color State, Date of death, Date of diagnosis, Days Left To Attempt Contact, DD-214, Death date, Death Date Time, Deceased Flag, demographics, Diagnosis, Discharge Date Time, Discharge Revocation Date, Dispositioned Date, DMII(Diabetes Mellitus Type 2), Electronic Data Interchange Personal Identifier (EDIPI), eligibility information, E-mail Address, Email Request Type, Email Sent At, Email Status, email Survey Finished At, enrollment information, Exam Appointment Information, exchanges Veteran demographics, Facility, File Number, financial assessment information, First Lab Chem Result Value, First Lab Chem Test Name, First Tested Positive, Follow Up Plan, had covid, had covid Label, Health Information, Hospitalization dates, Hospitalized, info receive care, info receive care Label, insurance, job Start Time(Job start time), jobId(Job Identifier), Laboratory results, Last Lab Chem Result Value, Last Lab Chem Test Name, Last Tested Positive, Latest Visit Date Time, LC Clinic Appointment, Letter Sent, Location Code, Next Primary Care Provider Appointment, opted-Out, Outpatient/inpatient clinic visit, Participant ID, Patient Aligned Care Team (PACT) Location, Patient ID, Patient SID (Patient Secondary Identifier), Patient Urban, Rural, Highly Rural geocode (URH), payment details, Physician name, Primary Care Provider Name, Private insurance status, receive care, receive care Label, Recorded Date, runId(Run Identifier), screener sent, sensitivity, service connection, Sex At Birth, social media account, Source Tables, Sta3n (Location of the VistA installation), survey Finished At, symptoms ladder, symptoms ladder Label, Telephony data, Text Request Type, Text Sent At, Text Status, text Survey Finished At, User Names, VA Demographics, VA Identifier, VA Participant ID, veteran feedback generated from Survey, veterans inquiries, VISN (Veteran Integrated Services Network), Vital Status, wants care, why no care, zip code.

PII Mapping of Components (Servers/Database)

Summit Data Platform consists of **34** key components servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Summit Data Platform** and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
CDW -1	Yes	Yes	Name, Social Security Number, Email, Health Information, Benefits Information, Claims Decision, DD-214, Mailing Address, Phone Number, Date of Birth	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -2	Yes	Yes	Name, Social Security Number, Email, Health Information, Benefits Information, Claims Decision, DD-214, Mailing Address, Phone Number, Date of Birth	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -3	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -4	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing	To ingest veteran data into the SDP	Role-based access granted

			address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	environment for data reporting and analytics purposes, and clinical care decision making	through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -5	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -6	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -7	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit

CDW -8	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -9	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -10	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -11	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted

					at rest and in transit
CDW -12	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -13	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -14	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -15	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care	Role-based access granted through the Elevated Privileges Access System (EPAS)

			records, race/ethnicity	decision making	•Data is encrypted at rest and in transit
CDW -16	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -17	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -18	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -19	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications,	To ingest veteran data into the SDP environment for data reporting and analytics	Role-based access granted through the Elevated Privileges Access

			previous medical records, race/ethnicity	purposes, and clinical care decision making	System (EPAS) •Data is encrypted at rest and in transit
CDW -20	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -21	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -22	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -23	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number,	To ingest veteran data into the SDP environment for data	Role-based access granted through the Elevated

			contact information, current medications, previous medical records, race/ethnicity	reporting and analytics purposes, and clinical care decision making	Privileges Access System (EPAS) •Data is encrypted at rest and in transit
CDW -24	Yes	Yes	Name, SSN, DOB, Mothers maiden name, mailing address, zip code, phone number, contact information, current medications, previous medical records, race/ethnicity	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
VA Profile	Yes	Yes	Name, VA Identifier, Phone Number, Email, Health Information, Benefits Information, Claims Decision, DD-214, Date of Birth	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
UDO CRM- D365	Yes	Yes	Customer Name, SSN, File Number, Customer VHA-generated documentation, Customer VBA-generated documentation, payment details, demographics, Personal Mailing Address, Contact History, Date of Birth, Electronic, Data Interchange Personal Identifier	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit

			(EDIPI), User Names, and Exam Appointment Information		
VA.GOV Chatbot (MS Dynamics Power Apps)	Yes	Yes	Name, SSN, DOB, Address, email, phone number, medical information	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
PATS-R (Patient Advocate Tracking System Replacement) MS D365	Yes	Yes	Veteran Integration Control Number (ICN), demographics, enrollment information, contact information, eligibility information, service connection, sensitivity, financial assessment information, and insurance, veteran feedback generated from Survey, Call Center, or Social Media, VA Demographics, and Case updates, veterans inquiries, complaints, and compliments	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
Member Services – Avaya servers (POM (SQL Server) & (WFO(SQL Server)	Yes	Yes	First Name, Last Name, SSN, DOB, Telephone Num	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care	Role-based access granted through the Elevated Privileges Access System (EPAS)

				decision making	•Data is encrypted at rest and in transit
CDWWork2 (Cerner DB)	Yes	Yes	Name, SSN, Date of birth, Race /ethnicity, Vital Status, Gender, City of residence, County of residence, Zip code, Hospitalization dates, Date of diagnosis, Date of death, Private insurance status, Laboratory results, Medications and therapies, Outpatient/inpatient clinic vis	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
BOSSPROD	Yes	Yes	DOB, Date of death, First name, Last name, Gender, Middle name, SSN, military status	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
BTSSS	Yes	Yes	First Name, Middle Name, Last Name, Patient ID, Veteran Integration Control Number (VAICN), Address, SSN, DOB, Telephone Number, Email address,	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
EDW (SQLDBPRODCxDW)	Yes	Yes	SSN, Full name, Birth date, Death	To ingest veteran data	Role-based access

			date, Electronic Data Interchange Personal ID, Race, Ethnicity, Gender, Diagnosis	into the SDP environment for data reporting and analytics purposes, and clinical care decision making	granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit
VEO DB (CDW Server)	Yes	Yes	Full Name, Email, Phone Number, Claim Info, Patient Id, Medical Records, SSN, DOB, social media account	To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making	Role-based access granted through the Elevated Privileges Access System (EPAS) •Data is encrypted at rest and in transit

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?
The Summit Data Platform (SDP) is a multi-cloud data enterprise data management and analytics platform that aggregates veteran data obtained from various disparate data sources across VA. These data sources include but are not limited to: Telephone Carriers, Interactive Voice Response (IVR), Automatic Call Distributors (ACD), Customer Relationship Management (CRM), White House Hotline, Survey Data, Corporate Data Warehouse and Palantir.

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.

Information from sources other than the individual is not required.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
SDP does not create information.

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?

Veteran data is ingested into SDP using the Golden Gate Replication, Azure Data Factory (ADF), Azure Copy, Athena, Synapse Pipeline, SFTP, and Qualtrics. The data sources are listed in response to question 1.2 above.

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

SDP does not collect directly from individuals.

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.

SDP is not an authoritative source but a downstream consumer of data from other authoritative systems. Accuracy is checked from the source systems.

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

Since SDP is not an authoritative source but a downstream consumer of data from other authoritative systems. However, reports could be developed to assist the field in identifying problems with data content in authoritative sources that the field can then go to the authoritative sources to correct. Data consistency verification is performed in the Azure Data Factory (ADF) to ensure the data is not only successfully copied from source to destination, but also verified to be consistent between source and destination store. If inconsistent files are found during the data movement, the copy activity is aborted. Data is checked for accuracy every time it's ingested to the SDP.

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

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

The applicable legal authority falls under SORN: 23VA10NB3: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111,501, 1151 1703, 1705, 1710, 1712, 1717,1720, 1721, 1724, 1725, 1727, 1728,1741–1743, 1781, 1786, 1787, 3102, 5701 (b) (6) (g) (2) (g) (4) (c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014 and SORN 54VA10NB3: Title 38, United States Code, sections 501 (a), 501 (b),1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101. Title 38 United States Code Section 7304, Rules and Regulations -Title 38 United States Code Section 501(b), and Deputy Secretary of Veterans Affairs - Title 38 United States Code Section 304.

Veterans Crisis Line Database- 158VA10NC5: 2015-09567.pdf (govinfo.gov)
Corporate Data Warehouse - 172VA10/ 86 FR 72688: 2021-27720.pdf (govinfo.gov)
Patient Medical Records – 24VA10A7: 2020-21426.pdf (govinfo.gov)
Mobile Application Platform (Cloud) Assessing (VAEC-MAP) – 173VA005OP2: 2021-24368.pdf (govinfo.gov)
Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA - 58VA21/22/28: 2019-02315.pdf (govinfo.gov)
Caregiver Support Program - Caregiver Record Management Application (CARMA) on Salesforce –197VA10: 2021-07310.pdf (govinfo.gov)
Veterans (Deceased) Headstone or Marker Records-VA (AMAS) – 48VA40B: 2023-09838.pdf (govinfo.gov)
Veterans and Dependents National Cemetery Interment Records-VA (BOSS) – 42VA41: 2023-01601.pdf (govinfo.gov)
Patient Advocate Tracking System Replacement (PATS-R)- VA-100VA10H: 2021-01501.pdf (govinfo.gov)
Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA-54VA10NB3: 2015-04312.pdf (govinfo.gov)
Non-VA Care (fee) Records-VA-23VA10NB3: 2015-18646.pdf (govinfo.gov)
Customer Relationship Management System (CRMS)-VA-155VA10/ 88 FR 63678: 2023-20044.pdf (govinfo.gov)
Personnel and Accounting Integrated Data System-VA-27VA047/77 FR 39346: 2012-16167.pdf (govinfo.gov)
Veterans Assistance Discharge System-VA- 45VA21/88 FR 7776: 2023-02388.pdf (govinfo.gov)
Community Placement Program-VA -65VA122/74 FR 33024: E9-16228.pdf (govinfo.gov)
Case and Correspondence Management-VA(CCM)-75VA001B/87 FR 36584: 2022-13066.pdf (govinfo.gov)
Veterans Health Information Systems and Technology Architecture (VistA) Records-VA-79VA10/85 FR 84114: 2020-28340.pdf (govinfo.gov)
Income Verification Records-VA-89VA10/88 FR 17639: 2023-05925.pdf (govinfo.gov)
Call Detail Records-VA-90VA194/74 FR 17283: E9-8448.pdf (govinfo.gov)

Telephone Service for Clinical Care Records [1]VA-113VA112/74 FR 21742: E9-10711.pdf (govinfo.gov)
The Revenue Program-Billing and Collections Records-VA-114VA10/86 FR 6996: 2021-01541.pdf (govinfo.gov)
MyHealtheVet Administrative Records-VA-147VA10/86 FR 46090: 2016-20217.pdf (govinfo.gov)
Enrollment and Eligibility Records-VA -- 147VA10/ 86 FR 46090: 2021-17528.pdf
Health Information Exchange–VA -- 168VA005/ 86 FR 6975: 2021-01516.pdf
HealthShare Referral Manager (HSRM)-VA -- 180VA10D/ 86 FR 46097: 2021-17527.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: PII/PHI of a veteran may not be relevant, accurate, complete, and current in the SDP system.

Mitigation: SDP is not a system of record and relies on the source (feeder) systems to ensure that PII collected is accurate, complete, and current. The following policies and procedures in the VA ensure that any PII collected and maintained by VA is accurate, relevant, timely, and complete for the purpose for which it is to be used:
•requires a veteran or an authorized representative to validate PII during the collection process
•when required, requests veteran or an authorized representative to revalidate that PII collected is still accurate
•confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information

•collects PII directly from the individual to the greatest extent practicable
•checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems; and
•issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Patient Identifier for SDP data consumers	Not used
Social Security Number	Patient Identifier for SDP data consumers	Not used
Date of Birth	Patient Identifier for SDP data consumers	Not used
Personal mailing address	Contact information for SDP data consumers	Not used
Personal phone number	Contact information for SDP data consumers	Not used
Personal Email address	Contact information for SDP data consumers	Not used
Emergency contact information	Contact information for SDP data consumers	Not used
Financial account information	Determine benefits for SDP data consumers	Not used
Health insurance beneficiary account number	Determine benefits for SDP data consumers	Not used
Current medication	Aid health decisions by SDP data consumers	Not used
Previous medical records	Aid health decisions by SDP data consumers	Not used
Race/ethnicity	Patient Identifier for SDP data consumers	Not used
Tax Identification Number	Patient Identifier for SDP data consumers	Not used
Medical record number	Patient Identifier for SDP data consumers	Not used

Gender	Patient Identifier and Aids health decisions by SDP data consumer	Not used
Military history/service connection	Aids health decisions by SDP data consumers	Not used
Biometrics	Patient Identifier for SDP data consumers	Not used
PHI	Aids health decisions by SDP data consumers	Not used
Activity tracker data, Admit Date Time, Age, Age range, Applicant Type, Benefits End Date, Benefits Information, Biometrics, bothering symptoms, bothering symptoms Label, Call Center, Caregiver ID, Caregiver Integration Control Number (ICN), Caregiver Status, Case updates, City of residence, Claims Decision, complaints, compliments, Consult, Contact History, contact information, County of residence, Covid 19 (U09_9) Date Assigned, COVID case information, Covid ICD10 Codes (international classification of diseases version 10), Customer Name, Customer VBA-generated documentation, Customer VHA-generated documentation, Dashboard Color State, Date of death, Date of diagnosis, Days Left To Attempt Contact, DD-214, Death date, Death Date Time, Deceased Flag, demographics, Diagnosis, Discharge Date Time, Discharge Revocation Date, Dispositioned Date, DMII(Diabetes Mellitus Type 2), Electronic Data Interchange Personal	Aids health decisions by SDP consumers	Not used

Identifier (EDIPI), eligibility information, E-mail Address, Email Request Type, Email Sent At, Email Status, email Survey Finished At, enrollment information, Exam Appointment Information, exchanges Veteran demographics, Facility, File Number, financial assessment information, First Lab Chem Result Value, First Lab Chem Test Name, First Tested Positive, Follow Up Plan, had covid, had covid Label, Health Information, Hospitalization dates, Hospitalized, info receive care, info receive care Label, insurance, job Start Time(Job start time), jobId(Job Identifier), Laboratory results, Last Lab Chem Result Value, Last Lab Chem Test Name, Last Tested Positive, Latest Visit Date Time, LC Clinic Appointment, Letter Sent, Location Code, Next Primary Care Provider Appointment, opted-Out, Outpatient/inpatient clinic visit, Participant ID, Patient Aligned Care Team (PACT) Location, Patient ID, Patient SID (Patient Secondary Identifier), Patient Urban, Rural, Highly Rural geocode (URH), payment details, Physician name, Primary Care Provider Name, Private insurance status, receive care, receive care Label, Recorded Date, runId(Run Identifier), screener sent, sensitivity, service connection, Sex At		

Birth, social media account, Source Tables, Sta3n (Location of the VistA installation), survey Finished At, symptoms ladder, symptoms ladder Label, Telephony data, Text Request Type, Text Sent At, Text Status, text Survey Finished At, User Names, VA Demographics, VA Identifier, VA Participant ID, veteran feedback generated from Survey, veterans inquiries, VISN (Veteran Integrated Services Network), Vital Status, wants care, why no care, zip code.		

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?
SDP is hosted in the Microsoft Azure GovCloud (MAG). Business Intelligence (BI) solutions from Microsoft are used to inspect, cleanse, transform and model veteran data to support decision-making.
• Azure Data Factory brings together all structured, unstructured, and semi-structured data (logs, files, and media) to Azure Data Lake Storage.
• Structureless datasets are cleaned, transformed and combined with structured data from operational databases or data warehouses in the VA with the help of Azure Databricks.
• Native connectors between Azure Databricks and Azure Synapse Analytics are leveraged to access and move data at scale.
• The Advanced Analytics Teams (data scientists and data analysts) take advantage of Azure Databricks to perform root cause determination and raw data analysis.
• Query and report veteran data in Power BI and Microsoft SQL Services Management Studio
• Palantir, a data science tool, used for predictive modeling.
• Immuta discovers, protects, and monitors an organization's data. The technology supports self-hosted, self-managed deployments for customers who store their data on-premises or in private clouds.

• VISN 9 Community Care Patient Tracker Tool, within the Veteran's Integrated Network (VISN) 9, is a comprehensive system that serves as a consolidated and standardized repository for tracking veteran transfers and ED/inpatient care in the community.
• Collibra, a Metadata Management tool to capture metadata for any connected datasets/repositories, manage both SDP Metadata and the Enterprise Data Catalog to make that information available to VA users through the Rockies Analytics Platform.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The system does not create or make available new or previously utilized information about an individual.

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?

PII data are encrypted and transmitted through a secure network. The entire SSN is hidden from users, and SDP ensures that PII data is only released to the intended individual.

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

PII data are encrypted and transmitted through a secure network. The entire SSN is hidden from users, and SDP ensures that PII data is only released to the intended individual.

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

PII data are encrypted and transmitted through a secure network. The entire SSN is hidden from users, and SDP ensures that PII data is only released to the intended individual.

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?

A role-based access control (RBAC) security approach is used to limit users only to the information needed to do their job and prevent them from accessing information that doesn't pertain to them.

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

A variety of user roles and Active Directory user groups, ranging from administrators to supervisors and D&A stakeholders (consume reports) will exist in the system.

2.4c Does access require manager approval?

Yes, Data owners are responsible for authorizing access to PII and leverage the safeguards implemented by SDP DevSecOps.

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

Regular users' access to the system is audit semi-annually and privilege users quarterly.

2.4e Who is responsible for assuring safeguards for the PII?
The SDP user profiles identified to date are listed, but not limited to the table below.

Roles	**Tools**
Business Owner	Power BI Reports
Project Manager	Power BI Reports
Business Analyst	Power BI Reports
Data Analyst	Azure Data Lake Storage – Read Only (RO) Azure Databricks – Read Write (R/W) Azure Synapse Analytics – R/W Azure Analysis Service – R/W Power BI – R/W Any other outside source of data – RO
Data Scientist	Azure Data Lake Storage – RO Azure Databricks – R/W Azure Synapse Analytics – R/W Azure Analysis Service – R/W Power BI – RO
BI Developer	Azure Synapse Analytics – R/W Azure Analysis Service – RO Power BI – R/W
Data Engineer	Azure Data Factory – R/W Azure Data Lake Storage – R/W Azure Synapse – R/W Azure Analysis – R/W Azure Databricks – R/W Power BI – RO
Database Administrator	Azure Active Directory – RO Azure Data Factory – R/W Azure Data Lake Storage – R/W Azure Synapse – R/W Azure Analysis – R/W
IAM Admin/AD Adm	Azure Active Directory – R/W
Other Report View	Power BI – Read On

Section 3. Retention of Information

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

3.1 What information is retained?

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

- Name

- Social Security Number
- Date of Birth
- Personal Mailing Address
- Personal Phone Number
- Personal Email Address
- Emergency Contact Information
- Financial Account Information
- Health Insurance Beneficiary Numbers Account numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Gender
- Military History/Service Connection
- Other Data Elements (list below)

Activity tracker data, Admit Date Time, Age, Age range, Applicant Type, Benefits End Date, Benefits Information, Biometrics, bothering symptoms, bothering symptoms Label, Call Center, Caregiver ID, Caregiver Integration Control Number (ICN), Caregiver Status, Case updates, City of residence, Claims Decision, complaints, compliments, Consult, Contact History, contact information, County of residence, Covid 19 (U09_9) Date Assigned, COVID case information, Covid ICD10 Codes (international classification of diseases version 10), Customer Name, Customer VBA-generated documentation, Customer VHA-generated documentation, Dashboard Color State, Date of death, Date of diagnosis, Days Left To Attempt Contact, DD-214, Death date, Death Date Time, Deceased Flag, demographics, Diagnosis, Discharge Date Time, Discharge Revocation Date, Dispositioned Date, DMII(Diabetes Mellitus Type 2), Electronic Data Interchange Personal Identifier (EDIPI), eligibility information, E-mail Address, Email Request Type, Email Sent At, Email Status, email Survey Finished At, enrollment information, Exam Appointment Information, exchanges Veteran demographics, Facility, File Number, financial assessment information, First Lab Chem Result Value, First Lab Chem Test Name, First Tested Positive, Follow Up Plan, had covid, had covid Label, Health Information, Hospitalization dates, Hospitalized, info receive care, info receive care Label, insurance, job Start Time(Job start time), jobId(Job Identifier), Laboratory results, Last Lab Chem Result Value, Last Lab Chem Test Name, Last Tested Positive, Latest Visit Date Time, LC Clinic Appointment, Letter Sent, Location Code, Next Primary Care Provider Appointment, opted-Out, Outpatient/inpatient clinic visit, Participant ID, Patient Aligned Care Team (PACT) Location, Patient ID, Patient SID (Patient Secondary Identifier), Patient Urban, Rural, Highly Rural geocode (URH), payment details, Physician name, Primary Care Provider Name, Private insurance status, receive care, receive care Label, Recorded Date, runId(Run Identifier), screener sent, sensitivity, service connection, Sex At Birth, social media account, Source Tables, Sta3n (Location of the VistA installation), survey Finished At, symptoms ladder, symptoms ladder Label, Telephony data, Text Request Type, Text Sent At, Text Status, text Survey Finished At, User Names, VA Demographics, VA Identifier, VA Participant ID, veteran feedback generated

from Survey, veterans inquiries, VISN (Veteran Integrated Services Network), Vital Status, wants care, why no care, zip code

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.*

Per the National Archives and Records Administration Request for Records Disposition Authority Records Schedule: DAA-GRS-2013-0005, Item 51, data is destroyed 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use. For VA, as well as SDP, data is retained as long as it's needed for business use. Publicly accessible link to RCS Records Control Schedules (RCS) | National Archives and rcs10-1.pdf (va.gov)

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

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

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

Yes

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

VHA Record Control Schedule 10-1: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

Series/Disposition Authority:
1180.17/ N1-15-06-2, item 18
1260.1/ N1-15-03-1, item 3
1250.1/DAA-0015 2018-0001, item 0001
2100.3/DAA-GRS-2013-0006-0004, item 31
6000.1/N1-15-91-6, item 1a, 1b, and 1d
6000.1/N1-15-91-7, item 1
6000.7/N1-15-87-4, item 2a

6000.8/N1-15-87-4, item 3a and 3b
6000.9/N1-15-87-4, item 4a
6010.1/DAA-0015-2016-0001-0001
6050.1/N1-15-94-6, item 1 and 2
7900/DAA-0015-2020-0001-0001

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.

SDP data will be deleted after decommissioning, following the Records Control Schedule (RCS 10-1), in compliance with VA policy, by logically deleting the stored data then overwriting the virtual drives with generic/dummy data to ensure no previous ghost/residual data can be restored. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.
https://www.va.gov/vapubs/search_action.cfm?dType=1

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.
Yes, access control policies and procedures implemented in VAEC MAG to minimize the use of PII for testing, training, and research. PHI and PII data are only processed in Staging and Production Env.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

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

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

Follow the format below:

Privacy Risk: Possibility of data breach is higher if retention of PII is longer.

Mitigation: To combat a data breach, SDP implements the same retention schedule as the source record. SDP relies on the data ingested from data sources. Old data are automatically archived based on retention schedule requirements.

SDP data will be deleted after decommissioning, following the Records Control Schedule (RCS 10-1), in compliance with VA policy, by physically deleting the stored data then overwriting the drives with generic/dummy data to ensure no previous ghost/residual data can be restored.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Quality and Patient Safety (Data Analytics Product Line)	Corporate Data Warehouse (CDW)	Name, Social Security Number, Email, Biometrics, Financial Information, Health Information, Benefits Information, Claims Decision, DD-214, Mailing Address, Phone Number, Date of Birth	Transmitted electronically TLS/SSL over communication HTTPS
Veterans Experience Office	VA/DoD Identity Repository (VADIR)	Name, SSN, DOB, VA Identifier, Personal Mailing Address, Personal Phone Number, Personal E-mail Address	Transmitted electronically TCPS
Veterans Experience Office	White House VA Hotline (WHHL) in Salesforce	Name, VA Identifier, Phone Number, Email, Health Information, Benefits Information, Claims Decision	Transmitted electronically HTTPS
Veterans Experience Office	Caregiver Records Management Application (CARMA) Salesforce	Discharge Revocation Date, Caregiver Status, Dispositioned Date, Applicant Type, Veteran Integration Control Number (ICN), Benefits End Date, Caregiver ID, Caregiver Integration Control Number (ICN)	SAFE data transfer
Office of the Under Secretary for Benefit	Customer Relationship Management Unified Desktop Optimization (CRM UD-O) (MS D365)	Customer name, SSN, File Number, Customer VHA-generated documentation, Customer VBA-generated documentation, payment details, demographics, Personal Mailing Address, Contact History, Date of Birth, Electronic Data Interchange Personal Identifier (EDIPI),	HTTPS

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*
		User Names, and Exam Appointment Information	
Veteran Experience Office	VA Profile (VA PRO)	Name, VA Identifier, Phone Number, Email, Health Information, Benefits Information, Claims Decision, DD-214, Date of Bir	Transmitted electronically
Veteran Health Administration, VA Central Office, VHA HC	Cisco Telephony	Telephony data, Name, Address, Phone Number, Email	Transmitted electronically TDS
Office of Enterprise Integration	Palantir Federal Cloud Service (Palantir)	Name, SSN, Mailing Address, Physical Address, Next-of-kin information, COVID case information, Patient ID, VA Identifier, Phone Number, Email, Health Information, Benefits Information, Claims Decision, DD-214, & Date of Birth	Transmitted electronically HTTPS
Patient Care Services	VistA – Imaging (IMAGE)	Name, Address, SSN, DOB, Physician name All data in DICOM (DICOM Library - Anonymize, Share, View DICOM files ONLINE)	Transmitted electronically
Veterans Experience Office	Patient Advocate Tracking System Replacement (PATS-R) MS D365	Veteran Integration Control Number (ICN), demographics, enrollment information, contact information, eligibility information, service connection, sensitivity, financial assessment information, and insurance, veteran feedback generated from Survey, Call Center, or Social Media, VA Demographics, and Case updates, veterans inquiries, complaints, and compliments, exchanges Veteran demographics, contact information, enrollment information, eligibility	Transmitted electronically

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*
		information, service connection, sensitivity, financial assessment information, and insurance	
Member Services	Avaya	First Name, Last Name, SSN, DOB, Telephone Number	Transmitted electronically
Veteran Experience Office	VA.GOV Chatbot (MS Dynamics Power Apps)	Name, SSN, DOB, Address, email, phone number, medical information	Transmitted electronically
Office of the Chief Technology Officer	Business sponsor: VHA Office of Healthcare Innovation and Learning Digital Health Platform (DHP)	Integration Control Number (ICN), Name, DOB, Last 4 of SSN, Activity tracker data	Transmitted electronically HTTPS
National Cemetery Administration	Burial Operations Support System – Enterprise (BOSS)	DOB, Date of date, First name, Last name, Gender, Middle name, SSN, military status	Transmitted electronically
Veterans Experience Office	Beneficiary Travel Self Service System (BTSSS)	First Name, Middle Name, Last Name, Patient ID, Veteran Integration Control Number (VAICN), Address, SSN, DOB, Telephone Number, Email address	Transmitted electronically HTTPS
Veteran Health Administration (VHA) Corporate Date Warehouse	Firearms and Substance Use Disorders (SUD)	Patient SID (Patient Identifier), Integration Control Number (ICN), Date of Death, Patient Medical Report, Medical note	Transmitted electronically Azure Import
Veterans Experience Office	Customer Interaction History and Service (CIHS)	Participant ID, Electronic Data Interchange Personal Identifier (EDIPI), VA Participant ID	A private endpoint API
Veterans Experience Office	Enterprise Data Warehouse (EDW)	SSN, Full name, Birth date, Death date, Electronic Data Interchange Personal Identifier (EDIPI), Race, Ethnicity, Gender, Diagnosis	HTTPS

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: If access to the system is not monitored, there may be unauthorized use or disclosure of the information in SDP.

Mitigation: All organizational use of SDP data is routinely monitored, tracked, and logged by the SDP technical team. VA personnel are trained on the authorized uses of SDP information as well as consequences of unauthorized use or sharing of PII. Related controls: AR-3, AR-4, AR-5, AR-8, AP-2, DI-1, DI-2, IP-1, TR-1 are implemented to protect and ensure the proper handling of PII.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
SAIC	VSignals	Name, Gender, E-mail Address, Date of birth, Age, Location Code, Phone number, Race/ Ethnicity	Site to Site (S2S), IPSEC Tunnel, Secure FTP	MOU/ISA
VA OIT	Qualtrics XM	Patient SID (Patient Secondary Identifier), Patient First Name, Patient Last Name, Patient SSN, Age, Age Range, Sex At Birth, Gender, Race, Ethnicity, Sta3n (Location of the VistA installation), Next Primary Care Provider Appointment, Mailing Address, Zip Code, Phone Number, Email Address, VISN (Veteran Integrated Services Network), Urban, Patient Urban, Rural, Highly Rural geocode (URH), Facility, Patient Aligned Care Team (PACT) Location, Primary Care Provider Name, Primary Care Provider First Name, Primary Care Provider Last Name, First Tested Positive, First Lab Chem Test Name, First Lab Chem Result Value, Last Tested Positive, Last Lab Chem Test Name, Last Lab Chem Result Value, Hospitalized, Admit Date Time, Discharge Date Time, DMII (Diabetes Mellitus Type 2), Covid 19 (U09_9) Date Assigned, Start Date, End Date, Progress, Finished, Recorded Date, had covid, had covid Label, bothering symptoms, bothering symptoms Label, receive	HTTPS (API)	N/A

		care, receive care Label, info receive care, info receive care Label, symptoms ladder, symptoms ladder Label, wants care, why no care, Email Status, Email Sent At, Email Request Type, email Survey Finished At, Text Status, Text Sent At, Text Request Type, text Survey Finished At, screener sent, Dashboard Color State, Days Left To Attempt Contact, Follow Up Plan, Latest Visit Date Time, Deceased Flag, Death Date Time, survey Finished At, Consult, LC Clinic Appointment, opted-Out, Covid ICD10 Codes (international classification of diseases version 10), Letter Sent, Source Tables, job Start Time(Job start time), runId(Run Identifier), job Id(Job Identifier), version		
Veterans Experience Office	Defense Manpower Data Center (DMDC)- Navy and Marine Core Deployment Data	Electronic Data Interchange Personal Identifier (EDIPI), SSN, Last Name, First Name, Middle Name, DOB	SAFE data transfer	MOU/ISA

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: If access to the system is not monitored, there may be unauthorized use or disclosure of the information in SDP.

Mitigation: All organizational use of SDP data is routinely monitored, tracked, and logged by the SDP technical team. VA personnel are trained on the authorized uses of SDP information as well as consequences of unauthorized use or sharing of PII. Related controls: AR-3, AR-4, AR-5, AR-8, AP-2, DI-1, DI-2, IP-1, TR-1 are implemented to protect and ensure the proper handling of PII.

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.

VHA Privacy Notice: Notice of Privacy Practices IB 10-163
VA Privacy Impact Assessment: https://www.oprm.va.gov/privacy/pia.aspx
VHA HANDBOOK 1605.04, Notice of Privacy Practices: 1605_04_HK_2015-10-07.pdf
VHA Directive 1605.01 D (2023-07-23) Privacy and Release of Information: 1605_01_D_2023-07-24 (1).pdf

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

No. SDP is a central repository of integrated data from one or more disparate sources. Data does not originate in the SDP data warehouse. Information is collected, or copied, from systems of record (SOR) across the VA such as CDW, telephone carriers, IVR, ACD, CRM, WHHL and survey data, and brought into the data warehouse.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

The source system is responsible for providing a Privacy Act statement anytime information is collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium. This requirement ensures that the individual is provided with sufficient information about the request for information to make an informed decision on whether to respond.

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.
At the time of collection, individuals can decline a request to provide information. For instance, individuals have the right to refuse to disclose their SSNs to the VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)).

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.
VHA Directive 1605.01, Privacy and Release Information directive list the rights to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations.

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> If a privacy notice is not provided to the subject of the records, the public would not be aware of the information collected about the subject of the record.

<u>Mitigation:</u> The VA mitigates this risk by ensuring that this PIA – which serves as notice that SDP exists, what information it contains, and the procedures in managing the information – is available

online per the requirements of the eGovernment Act of 2002, Publication. L. 107–347 §208 (b) (1) (B) (iii).

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.***

Members of the public are not allowed direct access to their information stored in SDP.

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)?

SDP is exempt from the access provision 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?

See record access procedure from SORN: Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

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.

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 8 states the rights of an individual to request an amendment to any information or records retrieved by the individual's name or other individually identifiable information contained in a VA system of records, as provided in 38 CFR 1.579 and 45 CFR. 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 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 1.5

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
Individuals are made aware of the procedures for correcting her or his information through the Privacy Act statement provided at the time of information collection.
See record access procedure from SORN: Individuals seeking information regarding access to and contesting of records in this system may write, call, or visit the VA facility location where they are or were employed or made contact.

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.
A formal redress procedure is provided through the VA facility location at which the individual was either employed or made contact.
See record access procedure from SORN: Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: The SDP system denies a veteran direct access, redress and correction of their record maintained in the system. This may result in inaccurate veteran information making its way into the system.

Mitigation: A veteran who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or who wants to review the contents of such a record, should submit a written request or apply in person to the VA health care facility (or directly to the VHA) where care was rendered. Inquiries should include the patient's full name, SSN, and return address.

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?
All SDP users must obtain VA clearance.

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?
Direct access to SDP data is strictly prohibited for external agencies.

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.
A role-based access control (RBAC) security approach is used to limit users only to the information needed to do their job and prevent them from accessing information that doesn't pertain to them. A variety of user roles, ranging from administrators to supervisors and D&A stakeholders (consume reports) will exist in the system. The SDP user profiles identified to date are listed in Section 2.3 above.

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 SDP data management implementation is a collaborative effort involving the D&A, contractors, data scientists, system owners, and data analysts. Contractors have access to the system and its PII to support their duties that include but are not limited to big data ingestion, preparation, orchestration and management.

D&A is responsible for ensuring that all contractors working on the SDP system are cleared using the VA background investigation process and obtain a Minimum Background Investigation (MBI). Contractors must sign Non-Disclosure Agreements (NDA) and necessary contractual requirements governing access and handling of Veteran data.

D&A leadership is required to ensure that all contractors interfacing with SDP data are adhering to VA policies and OMB Memorandum M-06-15 and OMB Memorandum M-06-16. According to OMB Memorandum M-17-15, OMB Memorandum M-06-16 is rescinded and captured within other policies and NIST standards (https://policy.cio.gov/rescissions-identity-management/). Necessary roles and responsibilities have been established to restrict certain users to different access levels.

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.

Department of Veterans Affairs (VA) offers privacy and security training through a state-of-the-art online Talent Management System (TMS). Veterans Health Administration (VHA) and Veterans Benefit Administration (VBA) employees and contractors who have access to Protected Health Information (PHI) are required to complete:

1.VA Privacy and Information Security Awareness and Rules of Behavior (TMS ID: 10176)
2. Privacy and Health Insurance Portability and Accountability (HIPAA) Training (TMS ID:10203)

VA requires all users to take these courses, so they would know what to do to keep information safe and help VA comply with federal laws about privacy and information security. These courses help users understand their roles and responsibilities for keeping information safe and ensure that individual who have access to PII are trained to handle it appropriately.

All VA personnel must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB). Acceptance obtained through electronic acknowledgment is tracked through the TMS system.

Role-based Training includes but is not limited to and based on the role of the user.
1.Information Assurance for Software Developers IT Software Developers (TMS ID: 1016925)
2.Information Security Role-Based Training for Data Managers (TMS ID: 1357084)

3.Information Security Role-Based Training for IT Project Managers (TMS ID: 64899)
4.Information Security Role-Based Training for IT Specialists (TMS ID: 3197)
5.Information Security Role-Based Training for Network Administrators (TMS ID: 1357083)
6.Information Security Role-Based Training for System Administrators (TMS ID: 1357076)
7.Information Security Role-Based Training for System Owners (TMS ID: 3867207)

VA contractors must complete the privacy and security training courses to gain access to VA information systems or VA sensitive information. To maintain their access, contractors must complete this training each year.

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:* 09-Mar-2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* Please provide response 09-Mar-2023
5. *The Authorization Termination Date:* 08-Mar-2025
6. *The Risk Review Completion Date:* 09-Mar-2023
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.
(Refer to question 3.3.1 of the PTA)
SDP uses a combination of Software as a service, Infrastructure as a Service, Platform as a Service, and Commercial-off-the-shelf software.

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

Yes. VA maintains ownership rights over data including PII.

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.

No, ancillary data is collected but only available to VA.

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.

Yes, VA is accountable for the security and privacy of data held by a cloud provider on their behalf as described in the SLA.

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).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.10.26 08:07:02 -04'00'

Privacy Officer, Tonya Facemire

Albertino M. Estacio 119921

Digitally signed by Albertino M. Estacio 119921
Date: 2023.10.26 13:56:58 -07'00'

Information Systems Security Officer, Albert Estacio

MANVENDRA JHALA

Digitally signed by MANVENDRA JHALA
Date: 2023.10.30 17:57:16 -04'00'

Information Systems Owner, Manvendra Jhala

APPENDIX A-6.1

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

VHA Privacy Notice: Notice of Privacy Practices IB 10-163
VA Privacy Impact Assessment: https://www.oprm.va.gov/privacy/pia.aspx
VHA HANDBOOK 1605.04, Notice of Privacy Practices: 1605_04_HK_2015-10-07.pdf
VHA Directive 1605.01 D (2023-07-23) Privacy and Release of Information: 1605_01_D_2023-07-24 (1).pdf

HELPFUL LINKS:

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

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

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

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

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