Privacy Impact Assessment for the VA IT System called:

Palantir Federal Cloud Service -E

VA Corporate

Office of Enterprise Integration

eMASS ID #1237

Date PIA submitted for review:

1/2/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Ryan Stiegman	Ryan.Stiegman@va.gov	202-461-6627
Information System Security Officer (ISSO)	David Jones	David.Jones9@va.gov	734-263-9622
Information System Owner	Harris Khan	harris.khan2@va.gov	703-789-7883

Abstract

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

Palantir Federal Cloud Services -e is an operational platform that is used to analyze data and inform decisions being made in various program offices of the VHA. The platform pulls data from a variety of source systems and enables the creation of data pipelines, analyses, and reports on the information. Datasets are generally updated 1-2x per day, rather than in real-time, because the information is not intended to be used for either emergency response scenarios or clinical point-of-care decisions. Source data is never updated, changed, or deleted. Derived datasets can also be saved to a user's selected workspace through manual or scheduled downloads.

Overview

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

1 General Description

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

This product is used by VA staff, primarily business and financial analyst personnel, as well as executive leadership for visibility of Enterprise Business Intelligence data. The system will enable VA to securely integrate timely data of any type, including patient-level health record information, hospital capacity data, and supply chain data.

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

Palantir Federal Cloud Services will be controlled by the Office of Enterprise Integration and operated by Palantir.

2. Information Collection and Sharing

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

60 million individuals associated with the VA, including Veterans, caregivers, and employees.

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

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

This system integrates information on Veteran population analytics, patient-level health record information, supply and operations, financial workflows, and business processes for usage in business workflows across the VA enterprise.

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

The platform enables individuals to use a diverse set of tools, including application building tools, workflow building tools, integrated analytics tools, and developer tools, to configure workflows for individual users. These workflows span across population analytics, healthcare operations, supply chain operations, and VA business process operations. The information shared conducted by the Palantir Platform is directly embedded into these workflows.

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

Yes

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

Yes, the Palantir Platform enables VA administrators to ensure data is appropriately access controlled and only available to authorized users. The data can be further secured proportionate to its sensitivity by applying granular, project-based access controls to restrict or grant dataset sharing capabilities. All access controls are centrally managed and governed by OIT, and are derived from VA Active Directory groups, NSSD permissions, and other approved VA access controls.

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

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

BAA, MOU/ISAs and SORNs: 172VA10 / 86 FR 72688 - VHA Corporate Data Warehouse - VA (published December 22, 2021); The VA System of Record Notice (VA SORN) Patient Medical Records

VA, SORN 24VA10A7 (Oct. 2, 2020) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

27VA047/ 77 FR 39346 -Personnel and Accounting Integrated Data System-VA (published July 2, 2012)

76VA05/ 65 FR 45131 - General Personnel Records (Title 38)-VA (July 20, 2000); 161VA10 / 88 FR 42005 - Veterans Health Administration Human Capital Management-VA (published June 28, 2023)

171VA056A/ 78 FR 63311 - Human Resources Information Systems Shared Service Center (HRIS SSC)-VA (published October 23, 2013)

147VA10 / 86 FR 46090 - Enrollment and Eligibility Records-VA (published August 17, 2021); 150VA10/ 88 FR 75387- Enterprise Identity and Demographics Records-VA (published November 2, 2023)

114VA10, The Revenue Program-Billing and Collection Records-VA (Published January 25, 2021)

23VA10NB3 - Non-VA Care (Fee) Records– VA (Published: 7-30-2015)

54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (Published: 3-3-2015)

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) – VA (Published December 23, 2020); Non-Health Data Analyses and Projections for VA Policy and Planning-VA(149VA008A) (Published January 25, 2021)

Health Program Evaluation--VA (107VA008B) (Published January 25, 2021); Veterans, Dependents of Veterans, and VA Beneficiary Survey Records – VA (43VA008) (Published January 25, 2021)

Veteran, Patient, Employee, and Volunteer Research and Development Project Records – VA (34VA10) (Published June 23, 2021).

I. What is the SORN?

SORNs: 172VA10 / 86 FR 72688 - VHA Corporate Data Warehouse - VA (published December 22, 2021); The VA System of Record Notice (VA SORN) Patient Medical Records

27VA047/ 77 FR 39346 -Personnel and Accounting Integrated Data System-VA (published July 2, 2012)

76VA05/ 65 FR 45131 - General Personnel Records (Title 38)-VA (July 20, 2000); 161VA10 / 88 FR 42005 - Veterans Health Administration Human Capital Management-VA (published June 28, 2023)

171VA056A/ 78 FR 63311 - Human Resources Information Systems Shared Service Center (HRIS SSC)-VA (published October 23, 2013)

147VA10 / 86 FR 46090 - Enrollment and Eligibility Records-VA (published August 17, 2021); 150VA10/ 88 FR 75387- Enterprise Identity and Demographics Records-VA (published November 2, 2023)

114VA10, The Revenue Program-Billing and Collection Records-VA (Published January 25, 2021)

23VA10NB3 - Non-VA Care (Fee) Records– VA (Published: 7-30-2015)

54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (Published: 3-3-2015)

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) – VA (Published December 23, 2020); Non-Health Data Analyses and Projections for VA Policy and Planning-VA(149VA008A) (Published January 25, 2021)

Health Program Evaluation--VA (107VA008B) (Published January 25, 2021); Veterans, Dependents of Veterans, and VA Beneficiary Survey Records – VA (43VA008) (Published January 25, 2021)

Veteran, Patient, Employee, and Volunteer Research and Development Project Records – VA (34VA10) (Published June 23, 2021).

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

The system is not in the process of being modified.

4. System Changes

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

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

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

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

Section 1. Characterization of the Information

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

1.1 Information collected, used, disseminated, created, or maintained in the system.

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series

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

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

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

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

- ☒ Name
- ☒ **Full** Social Security Number
- ☐ **Partial** Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)
- ☒ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account Numbers
- ☐ Certificate/License Numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☒ Medical Record Number
- ☒ Sex
- ☒ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☒ Next of Kin
- ☒ Date of Death
- ☐ Business Email Address
- ☒ Electronic Data Interchange Personal Identifier (EDIPI)
- ☐ Other Data Elements (List Below)

Other PII/PHI data elements: Employment Information, Veteran Service Information, VHA encounter information, Period of Service cohort and dates

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

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

Information is integrated from other VA source systems, public data sources, and 3rd party data purchase from Acxiom.

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

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

The purpose of the system is to integrate data from disparate VA systems to enable more comprehensive analysis and decision-making, while still retaining the ability to implement granular security and access controls across datasets. Information processed with the system will be used by analysts, engineers, logisticians, clinicians, and VA executives to inform the VA's response to delivery of Veteran care. The system will, in part, leverage publicly available information (e.g. case counts, publicly available mobility data, and population demographic data), along with VA information, to further the VA's assessment of the delivery of care and ensure that it is able to meet both its direct care responsibilities, but also those related to support for the broader healthcare community. The system also secure 3rd party data purchased from Acxiom to enable secure use of Veteran contact information for those Veterans without active relationship with VA. This purchased data, due to its sensitivity, is secured from other VA data and only available to a limited set of individuals authorized by VA.

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

Analyses and reports are created within the system by VA employees and contractors. This information is exported to other systems per system owner direction.

1.3 Methods of information collection

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

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

With limited exception, the information is integrated from various existing VA source systems and technology applications. Integrated data access is established to mirror the form, content, and permissioning of the source systems. Data is transmitted through encrypted channels to ensure security of sensitive information. Data checks are conducted at the ingestion level and at periodic intervals to ensure quality is maintained and tracked. VA leadership and program supervisors explicitly approve any ingress and egress of information to ensure it complies with all VA privacy and legal frameworks.

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?

The information is not collected on a form.

1.4 Information checks for accuracy, and how often will it be checked.

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

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

- The functionalities of the system enable manual creation, edits, or deletion of logs, thus enabling accuracy, relevance, timeliness, and completeness of that information. The Palantir SaaS Platform enables implementation of data health checks on the pipelines and alerting. These flexible health checks validate the quality of model inputs and change-over-time workflows to make sure the most recent version of PII is available. Validation and data cleansing will occur at the direction of VA project administrators during the creation of data source pipelines to ensure accuracy and fidelity of information sources mirrored from source systems and ingested into the platform.
- Data versioning will be used to provide metadata on data updates for version control and historical validation.
- VA SMEs can also create or implement specific dataset health checks, such as assessing the existence of certain values, null percentages, data schema checks, and adherence to custom business rules/logic.
- [3rd party data purchase from Acxiom] The Office of Data Governance and Analytics produces datasets backing VACOM. Purchased data remains isolated and will never be used to update the Veterans' official VA records.

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

No.

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

A completed Business Associate Agreement (BAA), FEDRAMP certification:

1.Title 40 US Code § 1401 (3), Clinger-Cohen Act of 1996, which directs the development and maintenance of IT architectures by federal agencies to maximize benefits within the federal government.

2.U.S. Code Title 38, Section 527, VA is required to gather data for the purposes of planning and evaluating VA programs

3.Government Performance and Results Act of 1993, designed to improve federal program effectiveness, enhance Congressional decision-making and strengthen internal controls.

4.44 U.S. Code § 3506(b)(2) §3511(a)(2)(D) and (b); Foundation of Evidence-Based policy-making Act of 2018 (HR 4174); and OMB M-19-23, guidance on carrying out the Foundations for Evidence-Based Policymaking Act.

5. SORNs: 172VA10 - VHA Corporate Data Warehouse - VA (published December 22, 2021); Patient Medical Records- 24VA10A7; 27VA047/ 77 FR 39346 - Personnel and Accounting Integrated Data System-VA; 76VA05/ 65 FR 45131 - General Personnel Records (Title 38)-VA; 161VA10 / 88 FR 42005 - Veterans Health Administration Human Capital Management-VA; 171VA056A/ 78 FR 63311 - Human Resources Information Systems Shared Service Center (HRIS SSC)-VA; 147VA10 / 86 FR 46090 - Enrollment and Eligibility Records-VA; 150VA10/ 88 FR 75387 – Enterprise Identity and Demographics Records - VA; 114VA10, The Revenue Program-Billing and Collection Records-VA; 23VA10NB3 - Non-VA Care (Fee) Records– VA; 54VA10NB3 - Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA; 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) – VA; Non-Health Data Analyses and Projections for VA Policy and Planning-VA (149VA008A); Health Program Evaluation--VA (107VA008B); Veterans, Dependents of Veterans, and VA Beneficiary Survey Records – VA (43VA008)

6.Legal authority from COVID - Public Law No: 116-136 (03/27/2020) Coronavirus Aid, Relief, and Economic Security Act or the CARES Act; H.R.6666 - COVID-19 Testing, Reaching, And Contacting Everyone (TRACE) Act and Presidential Executive Orders (EO).

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The risks to using PII/PHI data are:

- Over exposure of sensitive data to end-users (or applications) that do not carry a proportionate, justified need to know
- Failure to redact or limit sensitive fields when a minimized record view is appropriate toa given task or analysis
- Unwarranted export, malicious exfiltration, or other risk
- (Attempt at) repurposing sensitive personal information for purposes beyond the identified scope
- Data quality issues leading to false matching of records or failure to join records that should be associated
- Break down in remediation process to modify, correct, append, or expunge records requiring such actions

Mitigation:

- Data minimization: to the greatest extent possible, data ingestion will be limited to that which is necessary and proportionate to the needs of VA officials using the platform to support their core work.
- Purpose specification: data sources that are ingested and include sensitive information will be further restricted in the system using granular access control and permission rules. Access will be granted on role-based and/or purpose-based conditions to ensure limited exposure and minimize risk of misuse.
- Data Quality and Validation: data quality reviews will be built into the data ingestion process with periodic reviews & validation.

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
Address	Used for geospatial analyses and reporting (e.g., breakdowns of care by county) as well as approved outreach by VEO and OPIA.	Data element is used for identification for data matching when purchasing from a third-party vendor. Data is purchased to fill gaps in cohorts for population analytics and Veteran outreach.
Date of Birth (DOB)	Used for demographic analyses and reporting (e.g.,	Data element is used for identification for data matching

	breakdowns of care by age group).	when purchasing from a third-party vendor. Data is purchased to fill gaps in cohorts for population analytics and Veteran outreach.
Date of death	Used to filter to only living veterans for historical analyses and operational tools.	No External Use
Electronic Data Interchange-Personal Identifier (EDIPI)	Used as a patient identifier to link veterans with other data elements.	No External Use
Email	Used for approved outreach by VEO and OPIA.	Data element is used for identification for data matching when purchasing from a third-party vendor. Data is purchased to fill gaps in cohorts for population analytics and Veteran outreach.
Ethnicity/race	Used for demographic analyses and reporting.	Data element is used for identification for data matching when purchasing from a third-party vendor. Data is purchased to fill gaps in cohorts for population analytics and Veteran outreach.
Financial information	Used for supply and acquisition decision-making tools in the platform.	No External Use
Health insurance beneficiary number	Used as a patient identifier to link veterans with other data elements.	No External Use
Internal Control Number (ICN)	Used as a patient identifier to link veterans with other data elements.	No External Use
Military History/Service Connection	Used for demographic analyses and reporting (e.g., PACT Act reporting).	No External Use
Name	Used to identify the veteran for outreach and for hospital staff using the tooling.	Data element is used for identification for data matching when purchasing from a third party vendor. Data is purchased to fill gaps in cohorts for population analytics and Veteran outreach.
Next of Kin / Emergency Contact Information	Used for hospital staff when viewing Veteran record.	No External Use
Phone number	Used for approved outreach by VEO and OPIA.	Data element is used for identification for data matching

		when purchasing from a third-party vendor. Data is purchased to fill gaps in cohorts for population analytics and Veteran outreach.
Sex	Used for demographic analyses and reporting (e.g., breakdowns of care by sex).	Data element is used for identification for data matching when purchasing from a third-party vendor. Data is purchased to fill gaps in cohorts for population analytics and Veteran outreach.
Social Security Number (SSN)	Used as Veteran identifier (immediately hashed in the platform to limit visibility and use)	Data element is used for identification for data matching when purchasing from a third-party vendor. Data is purchased to fill gaps in cohorts for population analytics and Veteran outreach.
Veteran service information	Used for demographic analyses and reporting (e.g., PACT Act reporting).	No External Use
VHA encounter information	Used for healthcare analyses and reporting (eg. Cohorting Veterans by episodes of care)	No External Use
Period of Service cohort and dates	Used for demographic analyses and reporting (e.g., PACT Act reporting).	No External Use

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

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

- The Palantir SaaS Platform provides several tools to facilitate users' common analytical and logical operations in sequence.
- These tools allow users to explore & visualize data, debug data quality, and cleanse and transform data.
- For non-technical users, Contour is an application that enables users to perform advanced analysis, transformations, and aggregation or appending of datasets via a point-and-click interface.
- For technical users, Code Workbook is an application that allows users to analyze and transform data in common languages using an intuitive graphical interface.

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.

- Data Quality/Provenance – regarding any newly derived data, data lineage is automatically generated within Palantir SaaS Platform, which can help administrators trace data to its source and ensure appropriate compliance with data policies.
- Additionally, the implementation of self-propagating authorizations enables administrators to ensure downstream compliance.

2.3 How the information in the system is secured.
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Data in the COP is encrypted both in transit and at rest:

In Transit: All data transferred to, from, and within the COP is encrypted, without exception. This includes not only boundary-traversing traffic containing VA data, but also internal, intra-service communication. In addition, all external connections to the COP are only allowed over encrypted protocols and only encrypted HTTPS endpoints are exposed. These connections require TLS 1.2+.

At Rest: All storage layers (including object stores, datasets, block storage, and disk volumes) are secured with server-side encryption. This encryption is performed with a 256-bit symmetric key using the Advanced Encryption Standards (AES) in Galois Counter Mode (GCM) with built-in authentication, as recommended by NIST 800-38D.

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

For a user to see any sensitive data on the platform, they must have access to CDW SPatient, SStaff, and Full permissions. Request for this access is made through the VHA NDS Access Form for Health Operations. In this form, requestors must ensure that they select SPatient, SStaff, and Full data; they also sign an agreement to use sensitive data appropriately and in accordance with the CDW guidance and their request must be approved by a supervisor.

The platform additionally uses National Security SSN Database (NSSD) and the Locally Secure View (LSV) permissions frameworks – associated to a user's PIV account – used by the VHA Support Service Center (VSSC) and the Computerized Patient Record Service (CPRS) for data access control.

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

- The Business Associate Agreement (Agreement) is to establish requirements for US Department of Veterans Affairs, Office of Enterprise Integration and I3 Federal, LLC in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules ("HIPAA Rules"), 45 C.F.R. Parts 160 and 164, for the Use and Disclosure of Protected Health Information (PHI).
- Palantir FCS is a FedRAMP-authorized SaaS application which was issued its initial FedRAMP Authority To Operate (ATO) on December 4th, 2019. The system is hosted external to the VAEC on AWS US East/West, which is itself a FedRAMP-authorized IaaS hosting a diverse group of VA information systems.
- The Palantir Foundry platform is in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the
- FIPS 199 system security categorization (reference VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program, and the TIC Reference Architecture).

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

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:

<u>Principle of Transparency:</u> Is the PIA and SORN, if applicable, clear about the uses of the information?

<u>Principle of Use Limitation:</u> 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?

Access to PII will be determined and governed by the system owner, representatives from the office of the Chief Data Officer, and by system owners/data stewards of the specific data sources. The Palantir platform will enable a mix of security controls to be applied to specific fields and data elements in the platform, and/or inherit the security controls of a given source system to ensure that proper data protection is maintained throughout the use of the platform. Per question 1.3, the ingest of any data will need to be approved and documented by

the business owners of the application. Oversight will be conducted by the same body and the granular access controls of the Palantir platform can be made available to VA ISSO and supervisory authorities in conjunction with the policies outlined in the approved ATO.

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

Access Controls are documented in the Sensitive Data Justification document (available on request).

2.4c Does access require manager approval?

Some datasets have additional restrictions by request of the data owners. To gain access to these datasets, a user must request access on the platform and the access requests are sent to the data owners and platform administrators for their approval or declination. Any dataset can be restricted from all users except those approved by the data/business owner, when especially sensitive.

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

All data access requests are recorded in the systems in which they requested access. Additionally, audit logs are available for any actions taken in platform, including accessing PII data.

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

PII safeguards are a shared operational responsibility of the system Privacy Officer and ISSO, along with OIT and OEI. The Palantir engineering team will support configuration to implement such safeguards.

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*

For all elements in 1.1 (Name, Full 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, Medications, Medical Records, Race/Ethnicity, Medical Record Number, Sex, Integrated Control Number (ICN), Military History/Service Connection, Next of Kin, Date of Death, Electronic Data Interchange Personal Identifier (EDIPI)), Employment Information, Veteran Service Information, VHA encounter information, Period of Service cohort and dates, the information can be configured to be retained indefinitely or archived based on VA policy.

3.2 How long is information retained?

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

- In the Palantir SaaS Platform, retention policies can be set on datasets for configurable time periods to run automatically for only 1 year.
- These policies, and any changes to them, are tracked within the Palantir SaaS Platform.
- For data ingested directly from source systems, the Palantir SaaS Platform can be configured to mirror the retention rules of those systems, such that deletions will propagate through the Palantir SaaS Platform to the user frontend.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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

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

Yes, in accordance with VA Data Retention Policy.

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

The Data that is only stored for 1 year and will transport or transmit VA sensitive information is in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated. Additionally, firewall and Web services security controls meet VA minimum requirements.

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.

Data destruction is completed in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

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.

Palantir Technologies' employees are subject to the same security, training, and data access restrictions a customer requires for any other employee or contractor. Policies and procedures have been established to ensure responsibility and accountability (AR-1). Palantir Technologies has developed and implemented a comprehensive governance and privacy program that demonstrate organizational accountability for and commitment to the protection of individual privacy. Additionally, Palantir Technologies has a Data Protection Team and a Data Protection Officer focused on compliance with various privacy regimes. These teams are also responsible for communicating applicable requirements and supporting Palantir Technologies Senior Management and the CISO with enforcement of these policies. See Palantir Technologies' Privacy and Security Statement (https://www.palantir.com/privacy-and-security/) for more details (AR-1, AR-2).

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

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

Follow the format below:

Privacy Risk:

1. Preservation of data that is stale, invalid, or should have been previously expunged.
2. Information held beyond its appropriate lifecycle can misrepresent or provide inaccurate or data details about individual status.
3. Information that represents prior issues with, for example, mental health or substance abuse, that has not been appropriately expunged may create risks of stigmatization in the event of breach

Mitigation:

1. Review cycles for expungements – periodic data validation and expungement reviews will provide an opportunity to reassess data currency, validity, necessity and proportionality. Data that is deemed to be inaccurate or no longer necessary may be scheduled for systematic expungement.
2. Further flags will be identified for review of certain classes of sensitive data that may be subject to specific validity or other concerns/requirements motivating a tighter review and/or deletion schedule.
3. Data pipeline evaluations to ensure pipelines to source systems are being regularly updated such that source system expungements are being propagated downstream to the platform.
4. Information sources that are sensitive but may not meet immediate expungement criteria can, as needed, be further restricted using access controls and permissioning rules. This includes potential data archiving while data elements are being scheduled for upcoming review or deletion.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **Palantir Federal Cloud Service -E** consists of **2** 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 **Palantir Federal Cloud Service -E** and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application	Does this system collect PII? (Yes/No)	Does this system store	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

Program Interface (API) etc.) that contains PII/PHI		**PII? (Yes/No)**			
Management Plane/Information Security	Yes	Yes	• Address • Date of Birth (DOB) • Date of death • Electronic Data Interchange-Personal Identifier (EDIPI) • Email • Ethnicity/race • Financial information • Health insurance beneficiary number • Internal Control Number (ICN) • Military History/Service Connection • Name • Next of kin • Period of Service cohort and dates • Phone number • Sex • Social Security Number (SSN) • Veteran service information VHA encounter information	Information required by the program offices leveraging the platform	VA users are authenticated to the COP through VA's internal single sign on solution (SSOi), which requires use of a PIV Card (or a VA-approved PIV exemption) and enforces Multi-Factor Authentication (MFA.) As a part of the sign-on process, the platform pulls information about the user who is logging in, including the Active Directory (AD) groups that the user is a member of. The groups are used to mirror the VA's existing access control list (ACL) structures. There are additional controls to protect SSN information. The SSN is encrypted

					upon entry to the platform, with only select authorized users have permission to view the real SSN in "raw" tables, while all downstream tables use the encrypted SSN.
Palantir Federal Cloud Service Platform	Yes	Yes	• Address • Date of Birth (DOB) • Date of death • Electronic Data Interchange-Personal Identifier (EDIPI) • Email • Ethnicity/race • Financial information • Health insurance beneficiary number • Internal Control Number (ICN) • Military History/Service Connection • Name • Next of kin • Period of Service cohort and dates • Phone number • Sex • Social Security Number (SSN)	Information required by the program offices leveraging the platform	VA users are authenticated to the COP through VA's internal single sign on solution (SSOi), which requires use of a PIV Card (or a VA-approved PIV exemption) and enforces Multi-Factor Authentication (MFA.) As a part of the sign-on process, the platform pulls information about the user who is logging in, including the Active Directory (AD) groups that the user is a member of. The groups are used to mirror the

			• Veteran service information VHA encounter information		VA's existing access control list (ACL) structures. There are additional controls to protect SSN information. The SSN is encrypted upon entry to the platform, with only select authorized users have permission to view the real SSN in "raw" tables, while all downstream tables use the encrypted SSN.

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

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Veterans Health Administration Corporate Data Warehouse (CDW), Maximo, Integrated Funds Distribution Control Activity Point/Generic Inventory Package, Federal Procurement Data System, Medical Center Allocation System	VHA data is permissioned within the system for use in healthcare, acquisition, and supply chain operations workflows. All PHI/PII is secured using NSSD or NSD permissions.	• Names • Address • SSN • ICN • EDIPI • DOB • Financial Information • Phone Numbers • E-mail • Military History/Service Connection • Date of death • Health Insurance Beneficiary Number • Next of Kin • Employment Information	HTTPS over 443
Office of Acquisition and Logistics Product and Platform Management Tool, Virtual Office Acquisition, Enterprise Content Management System, Trigia, Contract Review Management System	Data from OAL is used in the Analytics, Data, and Decision Support Unified Platform (ADDS UP) configured on top of the Palantir platform to provide acquisition professional data-driven insights while making contracting decisions.	Financial Information	HTTPS over 443
Office of the Secretary Veterans	Historical data used to evaluate VA's	• Financial Information Name	HTTPS over 443

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
Emergency Medical Review Services	emergency readiness and response.		
Office of Management Financial Management System	Data is used for relevant acquisition and financial workflows on the Palantir Platform.	• Name • Social Security Number • (SSN) • Talent Management • System (TMS) ID • Financial Information • Electronic Data • Interchange-Personal • Identifier (EDIPI) • Internal Control Number (ICN) • Ethnicity/Race • Sex	HTTPS over 443
Caregivers Support Program Caregiver Records Management Application (CARMA) – Salesforce	Data is used by Caregiver Support Program (CSP) staff on the Palantir Platform to administer VHA's Program of General Caregiver Support Services (PGCSS) and Program of Comprehensive Assistance for Family Caregivers (PCAFC).	• Names • Address • SSN • ICN • EDIPI • DOB • Financial Information • Phone Numbers • E-mail • Military History/Service Connection • Date of Death • Health Insurance Beneficiary Number • Next of Kin • Employment Information	Site to Site VPN HTTPS over 443
HR Information System (HRIS) HR Smart	Data is used to create an authoritative "Employee object", which connects VA personnel to their specific job functions.	• Name Date of Birth (DOB)	HTTPS over 443
Veterans Experience Office	Data is used to create authoritative list of	• Names • Address	HTTPS over 443

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
VA Profile	Veterans with their contact and demographic information. Used for population analytics and outreach efforts.	• SSN • ICN • EDIPI • DOB • Financial Information • Phone Numbers • E-mail • Military History/Service Connection • Date of Death • Health Insurance Beneficiary Number • Next of Kin • Employment Information	
Office of Community Care Community Care Reimbursement Systems (CCRS) (AITC)	Data is used by the Office of Integrated Veterans Care (IVC) to evaluate claims reimbursements for Veteran care provided by community clinics.	• Names • Address • SSN • ICN • EDIPI • DOB • Financial Information • Phone Numbers • E-mail • Military History/Service Connection • Date of Death • Health Insurance Beneficiary Number • Next of Kin • Employment Information	HTTPS over 1433
Data Governance and Analytics USVETS	• VetPop Projection baseline estimates • Mortality analyses • Migration analyses • Mortality report • C&P report • VA utilization report	• Names • Address • SSN • ICN • EDIPI • DOB • Financial Information	Data sync from VSSC, HTTPS over 443

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
	• Other DGA reports, data stories and analyses • Responses to ad hoc request from VASec, VA offices, Congress, reports, state reps, VSOs, etc… • Shared data with Census, NCHS • Shared data with VHA Enrollment & Forecasting, VHA Suicide Prevention, VBA Actuary • Allow operations access to data on SAS/grid and research access via DART/VINCI • Feed data into the PACT Act Veteran cohort on COP • Feed data to the Person Object on COP, which is used by many offices with footprint on the COP	• Phone Numbers • E-mail • Military History/Service Connection • Date of death • Health Insurance Beneficiary Number • Next of Kin • Employment Information	
Office of Electronic Health Modernization (OEHRM) VA Operational Data Store (ODS)	Data is used for the P-CoVA application to help maintain oversight and perform quality assurance processes related to active medications during Cerner migrations.	• Military History/Service Connection • Social Security Number • (SSN) • Internal Control Number • (ICN) Electronic Data Interchange-Personal Identifier (EDIPI)	HTTPS over 443
Veterans Health Administration Veterans Health Information	Data is used for the P-CoVA application to help maintain oversight and perform quality assurance processes	• Military History/Service Connection • Social Security Number (SSN)	HTTPS over 443

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
Systems and Technology Architecture (VistA) extract for 130 VAMC's (VX130)	related to active medications during Cerner migrations.	• Internal Control Number (ICN) Electronic Data Interchange-Personal Identifier (EDIPI)	
VA-DoD Information Repository (VADIR) VA/DoD Identity Repository	Data is leveraged to create cohorts for population analytics and Veteran outreach.	Veteran service information including deployment dates and locations, combat indicators, disability indicators, rank	HTTPS over 443, Java database connectivity (JDBC)
Summit Data Platform (SDP) Summit	Data is used in creation of the "Person object", which is leveraged throughout the system to enable individuals to evaluate the care and services provided by the VA.	• Name • Address • Social Security Number (SSN) • Internal Control Number (ICN) Electronic Data Interchange-Personal Identifier (EDIPI)	Azure blob Filesystem Driver (ABFS)
Corporate Data Warehouse SAS_Grid	Data is used in creation of the "Person object", which is leveraged throughout the system to enable individuals to evaluate the care and services provided by the VA.	• Name • Address • Social Security Number (SSN) Data of death	Secure File Transfer Protocol (SFTP)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: If static data is leveraged, then the Palantir SaaS Platform may not be able to ascertain whether additions/deletions/changes have been made to the underlying source systems that contain PII

Mitigation:

- Administrators can use Palantir SaaS Platform features to notify users of applicable data use agreements, require user acknowledgements, or capture a user-provided justification prior to export from the platform. This metadata can be used to ensure purpose limitation and manage compliance with data auditing and oversight requirements.
- Additionally, incoming connections to Foundry are subject to strict IP whitelisting. VA will provide Palantir the IP range/CIDR block for your users & the Data Connector server.
- Additionally, the Identity and Access Management (IAM) Single Sign-On – Internal (SSOi) service is an authentication service specifically designed for controlling access for Department of Veterans Affairs (VA) internal users (employees and contractors) accessing VA applications. This service enhances the user experience by reducing the time associated with multiple log-on and log-off activities that require application-specific identifiers and passwords.
- The service also enables enriched password management and reduction in help desk support.
- Also, data pipeline evaluations to ensure pipelines to source systems are being regularly updated such that source system expungements are being propagated downstream to the platform.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
3rd Party Data Purchase – Axciom	Data is purchased to fill gaps in cohorts for population analytics and Veteran outreach.	• Name • Address • Social Security Number (SSN) • Date of Birth (DOB) • Demographic information • Phone number • Email	Contract	SFTP data transfer

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data within the Department of Veteran's Affairs could happen and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by the VA and Palantir personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within. Use of Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Palantir databases also reside in an AWS GovCloud (FEDRAMP certified), Palantir is a FEDRAMP certified product, Palantir has been granted a 3-year VA ATO, and has a BAA and MOU ISA in place with the VA documenting Palantir's agreement to safeguard the VA data. The data is also encrypted in transit using FIPS 140-2 security standards.

Section 6. Notice

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

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

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

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

A notice was not provided.

6.1b If notice was not provided, explain why.

No notice was provided because Palantir collects and integrates data from multiple VA sources and does not interact directly with individuals to collect data but data is reutilized in accordance with the source system authority therefore no notification is necessary (i.e., data corrections occur in sources system not Palantir. Palantir does not collect PII/PHI from individuals and instead will pull in data from databases on existing internal systems. Therefore, there is no requirement for Palantir to provide a notice to individuals.

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

No notice is provided.

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.

Palantir is not a system of record but can inherit the policies of the underlying source system by enabling granular security and access controls to be applied to the data and enforced on a per-user basis.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

A user would provide any right to consent to the underlying source systems of record.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

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

Privacy Risk: When data are transferred/exchanged from one system to another, it is possible that security permissions and policies about the use of information (security and policy metadata) are not also transferred.

Mitigation: VA System of record notice-PALANTIR
The VA will implement technical constraints on use of data at the data set level (or more granular) to ensure compliance with security and policy metadata and minimize internal exposure in cases of insufficient notice. This ensures that users are only able to see the data elements that they have been approved to see and Palantir's robust auditing capabilities can be used to confirm compliance.

Section 7. Access, Redress, and Correction

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

7.1 The procedures that allow individuals to gain access to their information.

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

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

The system meets Federal Information System Management Act 2014 (FISMA) security controls. The system complies with framework policies including Federal Risk and Authorization Management (FedRAMP) Moderate and Health Insurance Portability and Accountability Act (HIPAA). The system provides security and privacy protection that allows multiple levels of access for different users based on Role Based Access Controls (RBAC), Classification Based Access Controls (CBAC), and Access Control Lists (ACL). The system provides the ability to mask any data element (including part of a data element (e.g. first five digits of social security number) based on user privileges defined by RBAC, CBAC, and ACL. The system propagates access control and data security through all data, data engineering transformation, data objects, data in IDE, all logic used in transformations, and all output data from IDE. The system provides visibility of user access to and within the platform and retain an audit history of user access and actions for the duration of the contract. The system maintains a history of user activity per session. The system also provides alerts based on abnormal usage patterns (e.g., attempts by data consumers to access sensitive data without proper privileges).

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)?

Not applicable. The system is not exempt from 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?

The Palantir Foundry platform is in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the

FIPS 199 system security categorization (reference VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program, and the TIC Reference Architecture).

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

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

The Palantir SaaS Platform can be configured in order to capture any required explicit corrections or amendments requests of the relevant individuals, but changes will generally be captured in the underlying source systems of record and updated in the Palantir SaaS platform through set pipeline schedules.

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.

Palantir is not a system of record but can inherit any changes/deletions made to the underlying source systems. Notification would be at the behest of the source system of record owners.

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.

Palantir is not a system of record, so any formal redress or alternatives would take place in underlying source systems of record and updated in the Palantir SaaS platform.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: If static data is leveraged, then the Palantir SaaS Platform may not be able to ascertain whether additions/deletions/changes have been made to the underlying source systems that contain PII.

Mitigation: The VA will aim to implement continuously updating pipelines, where possible, to ensure that data in the Palantir SaaS Platform remains up-to-date and consistent with the underlying source system changes. In addition, Palantir's granular access controls ensure that access to specific data elements can be tracked and audited to ensure compliance.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

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

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

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

- Procedural/Administrative steps for overseeing systems access and data permissioning – the system leverages VA's own SSO solution to enable user access.
- To carry out organizational access determinations, the Palantir SaaS Platform provides highly configurable access controls that enable administrators to implement flexible, granular permissions for entire projects, datasets, or even specific rows or columns within a dataset.

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?

Users from other agencies will not have access to the system.

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

Roles are an additive form of security and are the primary way to give users access and capabilities on resources and data. Without any role on a given resource, a user will not be able to see even the existence of that resource. There are five standard roles:

• Owner: administer access to resource
• Editor: modify the resource
• Viewer: see the content of the resource
• Discoverer: see the existence (but not content) of the resource
• Exporter: can download the resource

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

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

Contractors are utilized for maintenance, engineering, and project specific workflow creation.

8.2c. Does the contractor have a signed confidentiality agreement? Contractors that view PII / PHI have the necessary clearances and are bound by the contract.

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

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

For specific data within the system, yes, there is a NDA process. NDA are reviewed by the Project Owner continuously. Contractors must have access to said PII in order to complete the workflows and ensure integrity, validation, and verification of the PII data.

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.

The system mirrors VA access policies, including Active Directory groups and NSSD permissions. Access to these permissions require privacy and security trainings as required and enforced by VA policy.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 3/13/2023
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 11/20/2023
5. *The Authorization Termination Date:* 11/20/2025
6. *The Risk Review Completion Date:* 11/20/2023
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.***

This system has an A&A.

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

This system is a Software as a Service (SaaS) that uses cloud technology. The system is currently FedRAMP Authorized and active on the FedRAMP Marketplace under FedRAMP ID FR1912671248.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (* ***Refer to question 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

VA retains all ownership rights over data, including PII. GS-35F-0086U 36C10B21F0353.

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.

Palantir collects logs of system activity to detect attacks and intrusions, unauthorized connections, deviations from the baseline configuration, and faults or malfunctions. This ancillary data can only be accessed by select individuals through a secured management plane, specifically for administering the platform. Access is governed by least-privilege Role-Based Access Control (RBAC). Please refer to specifics detailed in Palantir's FedRAMP System Security Plan (SSP).

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.

Platform security and governance is a shared responsibility. Palantir Federal Cloud Services (PFCS) is accredited at the FedRAMP High baseline and assumes responsibility for infrastructure and platform security as delineated in the PFCS SSP. VA has authority over platform governance, including user access management, data ownership and integrations, data security, and user permissions. The two organizations partner closely on risk management, change management, and managing organizational requirements. Please refer to specifics detailed in Palantir's FedRAMP System Security Plan (SSP).

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

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

The system does not use RPA.

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 they provided in this Privacy Impact Assessment is true and accurate.

RYAN STIEGMAN

Digitally signed by RYAN STIEGMAN
Date: 2025.03.31 07:09:35 -04'00'

Privacy Officer, Ryan Stiegman

Digitally signed by DAVID JONES
Date: 2025.03.31 07:33:16 -04'00'

Information System Security Officer, David Jones

HARRIS KHAN

Digitally signed by HARRIS KHAN
Date: 2025.03.31 08:29:52 -04'00'

Information System Owner, Harris Khan

APPENDIX A-6.1

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

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)