Privacy Impact Assessment for the VA IT System called:

Palantir Federal Cloud Service

Office of Enterprise Integration

Veterans Health Administration (VHA)

Date PIA submitted for review:

08/22/2022

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	Amberly Ferry	Amberly.Ferry@va.gov	(512) 326-6140

Abstract

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

Palantir Federal Cloud Service is an analytical platform that is used to analyze data and understand decisions being made in various program offices of the Veterans Health Administration (VHA). The primary users of the platform are analysts at the Veterans Integrated Service Network (VISN) and VA Central Office (VACO) levels of the organization to identify trends in care being provided to spark conversations and inform executive strategy.

Similar to many commercial BI business intelligence tools 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 PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

Palantir Federal Cloud Service is a cloud-hosted Software as a Service (SaaS) data integration and analytic platform for out-of-the-box immediate use by the Veterans Health Administration (VHA) to

track and analyze patient experience, supply and operations, financial workflows, and data quality across the VA enterprise. The SaaS platform is data agnostic and captures, curates, integrates, stores, searches, shares, transfers, performs deconfliction, analyzes, and visualizes large amounts of disparate structured and unstructured data. The SaaS platform architecture and suite of analytical tools allow users to perform intuitive, multi-dimensional analysis to reveal unseen patterns, connections, and trends across the VA health care system. The acquired SaaS data integration and analytic platform will enable VA to securely integrate near real-time updating data of any type, including: patient-level health record information, hospital capacity data, supply chain data, Veterans population data, and VA health care enrollee data. With the integrated data, the SaaS platform also enables users to exchange insights and decisions securely within the VA and externally with state, local, Federal, and private stakeholders via a suite of collaborative tools.

Sources of information include, but are not limited to:
Corporate Data Warehouse, Maximo, VA Information And Computing Infrastructure, Integrated Funds Distribution Control Activity Point, VHA Support Service Center, VistA, Product And Platform Management Tool, Contract Review Management System, Veterans Affairs Enterprise Cloud, Veterans Emergency Medical Services, Financial Management System, USVETS, VA Profile, Rockies, Caregivers Records Management Application (CARMA), HRSmart, Community Care Reimbursement Systems (CCRS), VADIR, Summit (SDP), and Electronic Contract Management System (eCMS), VA Video Connect (VVC), Text Integrated Utility (TIU) Notes. The full list of sources and data shared can be found in section 4.1 of this document.

At most, losing access to Palantir Federal Cloud Service would have a serious impact on the organization's ability to analyze and understand operational decisions at the leadership levels, but if this were the case, source systems would not be materially affected and could be leveraged.

The expected number of individuals whose information is stored in the system is 100+ with a connection to the Corporate Data Warehouse (CDW) and VistA. Individuals who utilize VA Health Care have information that may be stored in the system and this includes Veterans, Veteran family members, and VA emloyees. A completed Business Associate Agreement (BAA) and Federal Risk and Authorization Management Program (FEDRAMP) certification is available. The completion of this PIA will not result in circumstances that require changes to business processes nor technology changes.

Palantir Federal Cloud Service is a FedRAMP-authorized SaaS application that received initial FedRAMP Authority To Operate (ATO) on December 4th, 2019 and has an ATO High rating through May 27, 2023. The system is hosted external to the VA Enterprise Cloud (VAEC) on Amazon Web Services (AWS) US East/West, which is itself a FedRAMP-authorized IaaS hosting a diverse group of VA information systems.

Palantir Federal Cloud Service is in accordance with the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), the The National Institute of Standards and Technology (NIST), and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic private health information (PHI), outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with Federal Information Processing Standard (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).

Ultimately, Palantir Federal Cloud Service enables administrators at different sites across the VA to appropriately control access to data and ensure it is only available to authorized users. Administrators can use Palantir Federal Cloud Service to apply granular, project-based access controls to restrict or grant dataset sharing capabilities to further secure the data based on its sensitivity to ensure that all PHII/PII information is appropriately controlled IAW VA standards and permissions structure.

Palantir Federal Cloud Service's VA IT System is the Office of Information Technology (OIT).

Section 1. Characterization of the Information

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

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

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

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

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

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

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

☒ Other Unique Identifying Information (list below)

- VA Personal ID numbers (not Social Security Number (SSN)) for patients and/or employees
- Other primary/unique keys utilized by various VA systems

PII Mapping of Components

Palantir Federal Cloud Service consists of 2 key components (databases). 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 and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Management Plane/Information Security	Yes	Yes	User Logs (Social Security Number, Date of Birth, personal phone and email address, mother's maiden name, ethnicity, emergency contact, health insurance, medical record, current medication, previous medical records, other identifiers)	Information security	Access controls established that segregate duties, data minimization functions can be configured to limit exposure of PII in the platform, use of TLS 1.2 and FIPS 140-2 validated encryption for data at rest and in transit, monitoring and logging of account usage and system events, and malware detection.

Palantir Federal Cloud Service Platform	Yes	Yes	User Logs (Social Security Number, Date of Birth, personal phone and email address, mother's maiden name, ethnicity, emergency contact, health insurance, medical record, current medication, previous medical records, other identifiers)	VA use cases including, but not limited to, supply and operations, financial workflows, Veteran's access to care, Population Analytics and data quality across the VA enterprise	Access controls established that segregate duties, data minimization functions can be configured to limit exposure of PII in the platform, use of TLS 1.2 and FIPS 140-2 validated encryption for data at rest and in transit, monitoring and logging of account usage and system events, and malware detection.

1.2 What are the sources of the information in the system?

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Sources of information will include, but are not limited to:
Corporate Data Warehouse, Maximo, VA Information And Computing Infrastructure, Integrated Funds Distribution Control Activity Point, VHA Support Service Center, VistA, Product And Platform Management Tool, Contract Review Management System, Veterans Affairs Enterprise

Cloud, Veterans Emergency Medical Services, Financial Management System, USVETS, VA Profile, Rockies, Caregivers Records Management Application (CARMA), HRSmart, Community Care Reimbursement Systems (CCRS), VADIR, Summit (SDP), and Electronic Contract Management System (eCMS), VA Video Connect (VVC), Text Integrated Utility (TIU) Notes

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Palantir Federal Cloud Service allows the manual creation, edits, or deletion of logs, which ensures the accuracy, relevance, timeliness, and completeness of that information. The Palantir Federal Cloud Service 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 subject matter experts (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.

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

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: 172VA10A7- VHA Corporate Data Warehouse - VA (published August 25, 2020); The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Aug. 14, 2014) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.gpo.gov/fdsys/pkg/FR-2014-08-14/pdf/2014-19283.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); 161VA10A2/ 83 FR 11297 - Veterans Health Administration Human Capital Management-VA (published March 14, 2018); 171VA056A/ 78 FR 63311 - Human Resources Information Systems Shared Service Center (HRIS SSC)-VA (published October 23, 2013); 147VA10NF1/

81 FR 45597 - Enrollment and Eligibility Records-VA (published July 14, 2016); 150VA19/ 73 FR 72117 - Administrative Data Repository-VA (published November 26, 2008); 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); 24VA10A7: Patient Medical Records-VA, (Published: October 2, 2020); 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); Health Program Evaluation--VA (107VA008B); Veterans, Dependents of Veterans, and VA Beneficiary Survey Records – VA (43VA008); Veteran, Patient, Employee, and Volunteer Research and Development Project Records – VA (34VA10) (Published June 23, 2021)

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.

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: 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 to a given task or analysis.
- Unwarranted export, malicious exfiltration.

- Attempts to repurpose sensitive personal information beyond the identified scope.
- Data quality issues leading to false record matches or failure to join associated records.
- 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. All data sets have associated health checks to ensure data quality. These checks are run on schedules agreed to by VA and Palantir engineers.

Section 2. Uses of the Information

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

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

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

The information will be used in conjunction with the stated purpose in 1.1, which is to enable specific resource allocation decisions or guide medical policy planning for VA executives, analysts, and care providers.

Name: used to identify Veterans in the system.
Date of Birth: used to gather Veterans' age cohorts.
Mother's Maiden Name
Social Security Number: used to match Veterans' records across the platform for more comprehensive data.
Address: used for geolocation and population analyses.

Health Information: Used for analyses of Veteran population health conditions and healthcare experience.
Personal Phone Number: Used for population analyses of Veteran population and method of contact for Veterans
Personal Email Address: Used for method of contact for analyses of Veteran population
Emergency contact Information: Used for method of contact for analyses of Veteran population
Health Insurance Beneficiary Numbers: Used to support community care claims workflow
Race/Ethnicity: Used for analyses of Veteran population
Internet Protocol: Used to determine which services are available to Veteran
Gender: Used for analyses of Veteran population

2.2 What types of tools are used to analyze data and what type of data may be produced?

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The Palantir Federal Cloud Service SaaS Platform provides several tools to facilitate users' common analytical and logical operations in sequence. These tools allow users to explore and visualize data, debug data quality, and cleanse and transform data.

For non-technical users, Palantir Federal Cloud Service's 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, Palantir Federal Cloud Service's Code Workbook is an application that allows users to analyze and transform data in common languages using an intuitive graphical interface.

Data Quality/Provenance – regarding any newly derived data, data lineage is automatically generated within Palantir Federal Cloud Service SaaS Platform, which can help administrators trace data to its source and ensure appropriate compliance with data policies. The

implementation of self-propagating authorizations enables administrators to ensure downstream compliance.

2.3 How is the information in the system secured?

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

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

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

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

Data is encrypted in transit (FIPS 140-2 & TLS 1.2) and at rest (AWS KMS) to ensure security of sensitive information. All data leverages FIPS 140-2 validated cryptographic modules to encrypt data in transit and at rest.

Anytime an SSN is included in a dataset, the Palantir Federal Cloud Service team obfuscates (hashes) the SSN, replacing the SSN with a unique 128-character id after ingestion.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.</u>

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

<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.

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 Federal Cloud Service 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 business owners of the application must approve and

document the ingestion of any data. Oversight will be conducted by the same body and the granular access controls of the Palantir Federal Cloud Service platform can be made available to VA Information System Security Officer (ISSO) and supervisory authorities in conjunction with the policies outlined in the approved ATO.

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

In order for a user to see any sensitive data on the platform, they must have the following permission: CDW_spatient, CDW_sstaff, and CDW_full. Request for this access is made through the VHA National Data System (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 personal identification verification (PIV) account – used by the VHA Support Service Center (VSSC) and the Computerized Patient Record Service (CPRS) for data access control.

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

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: used to identify Veterans in the system.
- Date of Birth: used to gather Veterans' age cohorts.
- Mother's Maiden Name
- Social Security Number: used to match Veterans' records across the platform for more comprehensive data.
- Address: used for geolocation and population analyses.

- Health Information: Used for analyses of Veteran population health conditions and healthcare experience.
- Personal Phone Number: Used for population analyses and method of contact for analyses of Veteran population
- Personal Email Address: Used for method of contact for analyses of Veteran population
- Emergency contact Information: Used for method of contact for analyses of Veteran population
- Health Insurance Beneficiary Numbers: Used to support community care claims workflow
- Race/Ethnicity: Used for analyses of Veteran population
- Internet Protocol: Used to determine which services are available to Veteran
- Gender: Used for analyses of Veteran population

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

In the Palantir Federal Cloud Service 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 Federal Cloud Service SaaS Platform. For data ingested directly from source systems, the Palantir Federal Cloud Service SaaS Platform can be configured to mirror the retention rules of those systems, such that deletions will propagate through the Palantir Federal Cloud Service SaaS Platform to the user frontend.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

Records are maintained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States and the National Archives and Records Administration (NARA) and published in Agency Records Control Schedules. If the Archivist has not approved disposition authority for any records covered by the system notice, the System Owner will take immediate action to have the disposition of records in the system reviewed in accordance with VA Handbook 6300.1, Records Management Procedures. The records may not be destroyed until VA obtains an approved records disposition authority. See Records Control Schedule (RCS) 10–1 May 2016 for further detailed guidance. VA destroys electronic files when no longer needed for administrative, legal, audit, or other operational purposes consistent with the Record Control Schedule. In accordance with 36 CFR 1234.34, Destruction of Electronic Records, ‘‘electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules.’’

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?
This question is related to privacy control DM-2, Data Retention and Disposal

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. VA destroys electronic files when no longer needed for administrative, legal, audit, or other operational purposes consistent with the Record Control Schedule. In accordance with 36 CFR 1234.34, Destruction of Electronic Records, ‘‘electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules.’’ Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA Central Office (VACO) 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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Palantir does not use PII for research, testing, or training. Palantir is not used by research organizations such as HSR&D (Health Services Research and Development) or ORD (Office of Research and Development), but rather for operational decision making and thus the PHI and PII in it are not used for research purposes. In all tool training, Palantir uses deidentified data or dummy date to ensure no PII or PHI is shared. The training modules in Palantir consist of dummy data for sectors outside of healthcare so there is no chance of PII or PHI being shared. No testing occurs on the VA instance of the platform (testing occurs by the product team and they push updates) and thus VA data is not used for testing.

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.

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:

- Preservation of data that is stale, invalid, or should have been previously expunged
- Information held beyond its appropriate lifecycle can misrepresent or provide inaccurate or data details about individual status
- 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:

- 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.

- 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.
- 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.
- 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.

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Corporate Data Warehouse (CDW), Maximo, Integrated Funds Distribution Control Activity Point/Generic Inventory Package, Federal Procurement Data System, Medical Center Allocation System	Provides health care data to create health data objects	Asset data, workforce data, financial information, Name, date of birth, Social Security Number (SSN), race/ethnicity, Internal Control Number (ICN), diagnoses, previous medical records	TCP over 1443
Product and Platform Management Tool, Virtual Office Acquisition, Enterprise Content Management System, Trigia, Contract Review Management System	To present and assess VA supply chain trends and identify efficiencies and improvements	Financial information, construction and real property information, procurement data, contract data	HTTPS over 443
Veterans Emergency Medical Review Services	Veterans Emergency Medical Services data is needed for healthcare analyses	Financial information, staff name, staff ID	HTTPS over 443
Rockies	Office of Information Technology data platform. Used to create interoperable data environment and test interoperability	IT performance data, metadata	HTTPS over 443
Financial Management System	To analyze VA spending and acquisition patterns to identify efficiencies and improvements to be made.	Financial information, staff name, staff ID, Veteran billing, Veteran name, Social Security Number (SSN), Internal Control Number (ICN)	HTTPS over 443

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*
Caregiver Records Management Application (CARMA) – Salesforce	To support Caregiver Support Program (CSP) reporting	Veteran Caregiver data – including PII, Veteran PII (name, address, date of birth, Social Security Number (SSN), payment information, age, email, phone number, disability status and disability type), Caregiver application data, application appeal data, Veteran service information, Veteran need assessments, Caregiver award information,	Site to Site VPN and HTTPS over 443
HR Smart	To complete the employee object with authoritative data	Name, Date of Birth, ethnicity/race, sex/gender	HTTPS over 443
VA Profile	To complete the person objects with authoritative data and provide authoritative data for Caregivers analysis and reporting	Comprehensive Veteran care data, Name, SSN, Internal Control Number (ICN), EDIPI, contact information, mailing address, demographics, enrollment data, benefits data, military information/history, service-connected disability information	HTTPS over 443
Community Care Reimbursement Systems (CCRS) (AITC)	To create and enrich the Integrated Care Workspace	1. Medical Information 2. Provider Information 3. Claim information (identification, payments, reimbursements) 4. Eligibility information 5. Race/Ethnicity date of death 6. Family relationship 7. Eligibility 8. Disability rating 9. Gender 10. Next of Kin 11. Guardian 12. Employment information 13. Veteran dependent information 14. Death certificate information 15.	TCP over 1433

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*
		Name 16. Social Security Number 17. Date of Birth 18. Mailing Address 19. Zip code 20. Health Insurance Beneficiary Numbers.)	
USVETS2019	To enrich the data behind the person object	Comprehensive Veteran care data, name, SSN, ICN, EDIPI, contact information, demographics, enrollment data, benefits data, military information/history, service connected disability information	Data sync from VSSC, HTTPS over 443
VA Operational Data Store (ODS)	Data syndication and integration review and enterprise data model prototype	Immunizations, medications, names, ICN, SSN, patientSID	HTTPS over 443
Veterans Health Information Systems and Technology Architecture (VistA) extract for 130 VAMC's (VX130)	Data syndication and integration review and enterprise data model prototype	Immunizations, medications, names, ICN, SSN, patientSID	HTTPS over 443
VA/DoD Identity Repository	VA/DoD Identity Repository data is brought in for programs to analyze their data against DoD Person data, like military history.	Branch of Service, Character of Discharge, Discharge Data, War Era Served, Military History	HTTPS over 443, JDBC
Summit	To enrich data on individual Veterans and create joins to veteran object using SSN and/or Internal Control Number (ICN)	Name, Address, Social Security Number, Internal Control Number (ICN), Electronic Data Interchange Personal Identifier (EDIPI)	Azure Blob Filesystem Driver (ABFS)

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*
Electronic Contract Management System (eCMS)	Electronic Contract Management System is shared for the Category Management Support team to perform analysis on VA spending and investments. Only individuals associated with eCMS and with appropriate permissions can access this data due to contract sensitivity.	Accounting data, contract data, purchase card data, funding data, vendor information	Java Database Connectivity (JDBC)
SAS_Grid	To ingest USVETs data onto the COP to further enrich Veteran Data	VHA OPP Enrollment File, National Death Index, SSA Validation Master File	Secure File Transfer Protocol (SFTP)
Master Person Index (MPI)	Needed to ensure COP objects are based off authoritative person data	Integrated Care Number (ICN), Social Security Number (SSN), Full Name (first, middle, last), Veteran indicator, VA enrollment	JDBC
VA Video Connect (VVC)	To support the Accessing Telehealth through Local Area Stations (ATLAS) expansion pilot	Integrated Care Number (ICN), Social Security Number (SSN), Full Name (first, middle, last)	JDBC
Text Integrated Utility Notes (TIU)	Caregivers team to utilize data to assess the workload being completed for CSP program	TIU titles, status, and notes , which may contain PII or PHI around an individual or their medical conditions.	JDBC

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.
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 Federal Cloud Service 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 Federal Cloud Service 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 are subject to strict IP whitelisting. VA will provide Palantir Federal Cloud Service 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.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

The Palantir Federal Cloud Service Gotham connection is external to the VA; however, the CCRS connection is internal as it is between CCRS (AITC) and the Palantir Federal Cloud Service Data Connector inside the VA Enterprise Cloud (EC). Diagram below depicts this distinction. CCRS agreement is documented for the record.

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***
Palantir Federal Cloud Service Gotham for Enterprise Data Management on AWS	Data Analytics	Name, Address, Social Security Number, Internal Control Number (Internal Control Number (ICN)), Electronic Data Interchange Personal Identifier (EDIPI), Health and Human Services data, Census data	BAA MOU ISAs	FIPS 140-2 encrypted HTTPS over 443
Community Care Reimbursement System (CCRS)	Office of Community Care (OCC)	Claims data, Comprehensive Veteran care data, Veteran Name, Veteran ID	MOU ISA	TCP over 1433

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:
Privacy Risk: The privacy risk associated with 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 Federal Cloud Service 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 Federal Cloud Service databases also reside in an AWS GovCloud (FEDRAMP certified), Palantir Federal Cloud Service is a FEDRAMP certified product, Palantir Federal Cloud Service has been granted a 3-year VA ATO and has a BAA and Memorandum of Understanding (MOU) Interconnection Security Agreement (ISA) in place with the VA documenting Palantir Federal Cloud Service'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 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

No notice was provided because Palantir Federal Cloud Service 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 Federal Cloud Service. Palantir Federal Cloud Service 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 Federal Cloud Service to provide a notice to individuals.

SORNs: 172VA10A7- VHA Corporate Data Warehouse - VA (published August 25, 2020); The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Aug. 14, 2014) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.gpo.gov/fdsys/pkg/FR-2014-08-14/pdf/2014-19283.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); 161VA10A2/ 83 FR 11297 - Veterans Health Administration Human Capital Management-VA (published March 14, 2018); 171VA056A/ 78 FR 63311 - Human Resources Information Systems Shared Service Center (HRIS SSC)-VA (published October 23, 2013); 147VA10NF1/ 81 FR 45597 - Enrollment and Eligibility Records-VA (published July 14, 2016); 150VA19/ 73 FR 72117 - Administrative Data Repository-VA (published November 26, 2008); 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); 24VA10A7: Patient Medical Records-VA, (Published: October 2, 2020); 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); Health Program Evaluation--VA (107VA008B); Veterans, Dependents of Veterans, and VA Beneficiary Survey Records – VA (43VA008); Veteran, Patient, Employee, and Volunteer Research and Development Project Records – VA (34VA10) (Published June 23, 2021)

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

Information is not collected directly from individuals and put into Palantir Federal Cloud Service. Palantir Federal Cloud Service 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. Palantir Federal Cloud Service is not a source system for data. All other inquiries must be handled at the source system level.

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. Palantir Federal Cloud Service is not a source system for data. All other inquiries must be handled at the source system level.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

Principle of Transparency: Has sufficient notice been provided to the individual?

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

Follow the format below:
Privacy Risk: When data is 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 FEDERAL CLOUD SERVICE
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 Federal Cloud Service'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 What are the procedures that allow individuals to gain access to their information?

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

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

The Palantir Federal Cloud Service 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 Federal Cloud Service 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 Federal Cloud Service 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 Federal Cloud Service 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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

Incoming connections to are subject to strict IP whitelisting. Your organization should provide Palantir Federal Cloud Service the IP range/CIDR block for your users and 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.

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.

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: If static data is leveraged, then the Palantir Federal Cloud Service 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 Federal Cloud Service SaaS Platform remains up-to-date and consistent with the underlying source system changes. In addition, Palantir Federal Cloud Service'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.

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

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

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

- Procedural/Administrative steps for overseeing systems access and data permissioning – Palantir Federal Cloud Service will leverage the VA's own SSO solution to enable user access, so it can support existing VA data approval processes that utilize AD.
- To carry out organizational access determinations, the Palantir Federal Cloud Service 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. The implementation of self-propagating authorizations enables administrators to ensure downstream compliance.
- Users are individually given access to the platform after undergoing training and must be part of specific Active Directory (AD) groups to access specific data on the platform.

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.

Palantir Federal Cloud Service engineers and other contract staff will have access to PHI/PII in order to create data pipelines and products and use or maintain the system. All contractors must undergo VA's privacy training and will have to have CDW national PII/PHI permissions at the least to see PII or PHI.

Palantir Federal Cloud Service engineers and other contract staff will sign NDAs to access eCMS data specific to VA financial and acquisition work. The practice of signing NDAs can also be set up with any office sharing data on Palantir Federal Cloud Service if they request it.

Palantir Federal Cloud Service has completed a Business Associate Agreement (BAA) with the Department of Veterans Affairs, stating PHI is the property of VA and may not be used or disclosed outside of VA's direction.

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.

- Standard policy training, including VA training on HIPPA and PII policies (system and data security, and the VA Rule of Behavior)
- Palantir Federal Cloud Service specific training covering any details on security, privacy, and data permissioning in standard workflows

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Yes. The Security Plan was approved on November 12, 2021. A 3-year, full High ATO was approved October 22, 2020 through May 27, 2023. The Risk Review was completed on March 22, 2022. The FIPS 199 classification of the system is rated high.

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).

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

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

Yes, Palantir Federal Cloud Service uses Amazon Web Services (AWS), which is FedRAMP Authorized. Palantir Federal Cloud Services is not hosted within the VA Enterprise Cloud VAEC boundary.

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The VA has its own contract and relationship with AWS (36C10B19R0046). VA also has a Business Associate Agreement (BAA) with Palantir Federal Cloud Service (Non-VA Subcontractor Business Associate Agreement_OEI_I3 Federal S Final (Signed).pdf) which establishes the Department of Veterans Affairs as the owners of all PHI in Palantir Federal Cloud Service.

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 Federal Cloud Service has user and activity logs, VA metadata, and its own metadata, which are also considered VA data and will be owned by the VA in the event of contract termination or end of the contract.

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.

The BAA establishes VA's ownership of all data. This ownership is also stated in the Memorandum of Understanding between the VA and Palantir Federal Cloud Service. VA has also taken additional measures to establish all security practices around COP data access, audit security measures, and developed a white paper with thorough details on data security on the Palantir Federal Cloud Service platform (referred to as "The Common Operating Platform (COP)" at VA) as they hold responsibility for the security of the VA's data. This ownership is stated in all documentation to document the agreement that all VA data that enters Palantir Federal Cloud Service is VA property and will be returned to VA and not used any further by Palantir Federal Cloud Service upon the termination or end of the contract.

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**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Ryan J. Stiegman 166494

Digitally signed by Ryan J. Stiegman 166494
Date: 2022.09.14 15:44:33 -04'00'

Privacy Officer, Ryan Stiegman

DAVID T. JONES 3437864

Digitally signed by DAVID T. JONES 3437864
Date: 2022.09.14 15:36:27 -04'00'

Information Systems Security Officer, David Jones

AMBERLY FERRY

Digitally signed by AMBERLY FERRY
Date: 2022.09.14 14:22:22 -05'00'

Information Systems Owner, Amberly Ferry

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).

SORNs: 172VA10A7- VHA Corporate Data Warehouse - VA (published August 25, 2020); The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Aug. 14, 2014) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.gpo.gov/fdsys/pkg/FR-2014-08-14/pdf/2014-19283.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); 161VA10A2/ 83 FR 11297 - Veterans Health Administration Human Capital Management-VA (published March 14, 2018); 171VA056A/ 78 FR 63311 - Human Resources Information Systems Shared Service Center (HRIS SSC)-VA (published October 23, 2013); 147VA10NF1/ 81 FR 45597 - Enrollment and Eligibility Records-VA (published July 14, 2016); 150VA19/ 73 FR 72117 - Administrative Data Repository-VA (published November 26, 2008); 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); 24VA10A7: Patient Medical Records-VA, (Published: October 2, 2020); 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); Health Program Evaluation--VA (107VA008B); Veterans, Dependents of Veterans, and VA Beneficiary Survey Records – VA (43VA008); Veteran, Patient, Employee, and Volunteer Research and Development Project Records – VA (34VA10) (Published June 23, 2021) https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf