Privacy Impact Assessment for the VA IT System called:

Revenue Operations Payer Compliance Tool

Office of Finance

Revenue Operations

1193

Date PIA submitted for review:

04/15/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rhonda Spry-Womack	rhonda.spry@va.gov	615-613-2886
Information System Security Officer (ISSO)	Mark Farris	mark.farris@va.gov	(321) 320-0370
Information System Owner	Lori Franklin	lori.franklin@va.gov	813-792-8493

Abstract

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

The Office of Finance, Revenue Operations Program supports management of VHA revenue collections. As part of that effort, it uses standardize methods, tools, and processes to improve efficiency, effectiveness, and accountability. One such tool is the commercial off the shelf (COTs) Revenue Operations Payer Compliance Tool (ROPCT), is a **third-party** insurance account and payment data exploration tool. It provides scenario modeling and automatic calculation of insurance carrier agreements that compare actual reimbursements to expected payments and quantifies underpayments. ROPCT provides reports with various views, filters, customization, and search capabilities at the claim, VAMC, VISN, CPAC, and national level.

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?
Revenue Operations Payer Compliance Tool (ROPCT) – VHA Office of Finance, Revenue Operations

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
The ROPCT is an account and payment data exploration and analysis tool using a Software-as-a-Service (SaaS) solution hosted by MD Clarity. MD Clarity enables the identification of systemic patterns that result in incorrect allowable rates based on contractual agreements with payers. Given the complexity of today's payer provider contract terms and ever-changing payer reimbursement methodologies and policies, the level of sophistication built into MD Clarity's automated analysis is essential to monitoring the accuracy of payments the healthcare system receives. By using this kind of analysis, healthcare organizations will increase net revenue and more confidently validate future payments as contracts and payer policies change over time.

C. Who is the owner or control of the IT system or project?
Lori Franklin

2. Information Collection and Sharing

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

The typical affected individual is a Veteran who is eligible to receive care from the Veteran Administration (VA) Medical Center or from a community provider when the VA cannot provide the care needed. This care is provided on behalf of and paid for by VA. The expected number of individuals whose information is stored is 7.8 million.

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

The ROPCT system manages Veteran data extracted nightly from VistA, the VHA Financial Service Center (FSC), and Medispan.

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

Information in the ROPCT is received from VistA, FSC, and Corporate Data Warehouse (CDW). Information from ROPCT is shared to the Enterprise Denial Database, Workflow Tool, and mPOWER.

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

The ROPCT is not a system of record about Veterans. The ROPCT is only used to assist with processing of information related to VHA revenue operations. The application serves 7 Consolidated Patient Account Centers (CPACs) and 4 Regions within the VA. VA data resides inside the VA network on VA servers.

3. Legal Authority and SORN

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

Legal authority to operate the system can be found in Title 38, United States Code (U.S.C) 1729 which authorized the Department of VA to seek reimbursement from third-party health for the cost of medical care furnished to insured non-service-connected Veterans and create the means test copayments.

The legal authorities that defined the collection of information include Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

Systems of Records Notices applicable to this system are: 114VA10 / 86 FR 6996 The Revenue Program-Billing and Collections Records-VA. CFR › Title 38 › Chapter I › Part 3 › Subpart A › Section 3.216 – Mandatory disclosure of social security numbers. CFR › Title 38 › Chapter I › Part 1 › 38 CFR 1.575 - Social security numbers in veterans' benefits matters. U.S. Code › Title 38 › Part IV › Chapter 51 › Subchapter I › § 5101 38 U.S. Code § 5101 - Claims and forms CFR › Title 32 › Subtitle A › Chapter VII › Subchapter A › Part 806b › Subpart C › Section 806b.12 32 CFR 806b.12 –

Version Date: March 30, 2020, Page 4 of 28 Requesting the Social Security Number Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules.

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

The System of Records Notice (SORN) will not need to be modified. The system falls within the 114VA10 / 86 FR 6996 The Revenue Program-Billing and Collections Records-VA.

4. System Changes

J. Will the completion of this PIA will result in circumstances that require changes to business processes?
The completion of this PIA will not result in circumstances that require changes to business processes.

K. Will the completion of this PIA could potentially result in technology changes?
The completion of this PIA will not result in technology changes.

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. 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
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers

☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Other Data Elements (list below)

Other PII/PHI data elements: Employer, Diagnosis codes, Procedure codes, Date Last Seen, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Medications, Provider Name, Subscriber identification number.

PII Mapping of Components (Servers/Database)

ROPCT consists of **one** key component (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 **ROPCT** 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 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Workflow tool: Payer Compliance Tool (PCT) **PayerCompliance Database:**	**Yes**	**Yes**	**Stores all integrated VistA, 835 and Insurance Contract Data. Patient Name, SSN, DOB, Address, Sex, Employer, Diagnosis codes,**	**For the system to function and to accurately identify Veteran accounts for the purpose**	**Encryption, VA firewall hosted in FISMA Moderate environment. Access is limited to only those**

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

1. Payer Compliance Prod 2. Payer Compliance Test 1 3. Payer Compliance Test 2			**Procedure codes, Date Last Seen, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Medications, Provider Name, Subscriber identification number**	**of revenue collection activities**	**components required in the performance of work. Access is controlled by a series of access and verify codes and is only accessible via 2 factor authentications**

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

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

The sources of information are the Veteran's Health Information Systems and Technology Architecture (VistA), the VHA Financial Service Center (FSC), and VHA mobile Performance and Operational Web-enabled Reports (mPOWER)

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 individual does not interact with our system.

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

No data is being changed after it is extracted from VistA. The tool does not create or make available new or previously unutilized information about an individual.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from

another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

The information is extracted and received via electronic transmission from VistA, and the VHA Financial Service Center (FSC).
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?
OMB Approved No. 2900-0091
VA Form 10-10EZ

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

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

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

Each morning prior to the import of information, various checks are run against each of the VistA extracts received. These checks evaluate the integrity of a file to make sure there were no errors during the extract or transmission of the data. As part of this process, there is a designated Information Technology staff member that confirms each file is received as required. In addition, each CPAC has a designated coordinator with access to a daily import report that will alert them to import issues or possibly re-imported data files.
In addition to the manual review, there are also numerous checks in place that will notify stakeholders in the event of a job processing failure. These are often tied to behind-the-scenes system performance checks that help ensure the overall integrity of data within the system and related system performance. Lastly, there is also a process in place that allows end users of the ROPCT to elevate any data concerns experienced while utilizing the ROPCT for further research and validation.

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?

An aggregator is ROPCT's sole source of information.

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

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in

addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The legal authorities that defined the collection of information include Veteran Benefit Act, Chapter 73: Veterans Health Administration – Organization and Functions, Title 38, U.S.C. 7301 and U.S.C. 1729.

Privacy Act of 1974 - 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

Freedom of Information Act (FOIA) 5 USC 552

VA Directive 6500 Managing Information Security Risk: VA Information Security Program

Systems of Records Notices applicable to this system are:

114VA10 / 86 FR 6996 The Revenue Program-Billing and Collections Records-VA.

CFR › Title 38 › Chapter I › Part 3 › Subpart A › Section 3.216 - Mandatory disclosure of social security numbers. CFR › Title 38 › Chapter I › Part 1 › 38 CFR 1.575 - Social security numbers in veterans' benefits matters. U.S. Code › Title 38 › Part IV › Chapter 51 › Subchapter I › § 5101 38 U.S. Code § 5101 - Claims and forms CFR › Title 32 › Subtitle A › Chapter VII › Subchapter A › Part 806b › Subpart C › Section 806b.12 32 CFR 806b.12 - Requesting the Social Security Number Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules **1.6**

PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The ROPCT collects both Personally Identifiable Information (PII) and limited other Sensitive Personal Information (SPI) such as financial information. Due to the sensitive nature of this information, there is a risk that access by an unauthorized person could result in serious personal, professional, or financial harm to the individual to whom the information pertains.

Mitigation: Mitigations include the system being kept on the VA network, behind a VA firewall, with encryption of the databases, and the implementation of VA SSO, integrated. Access to PII is limited by the ROPCT to only those applications necessary for staff to perform their job, as determined by their management team and their job description. User roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles are determined by supervisors or higher. Users access is provided by CPAC OI&T following receipt of request from appropriate individuals.

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.

All information is for official internal use only and is collected, maintained, and processed for the following purposes:

- To process third party health insurance billing
- Enable supervisors to monitor activities and perform quality checks on work items
- Provide reporting capabilities that encompass all CPAC revenue cycle functions
- Produce reimbursement reports by insurance carrier by facility, region, or national
- Analyze insurance carrier reimbursement and performance

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
Patient Name	Veteran identification	Not used
Social Security Number	Veteran identification	Not used
Date of Birth	Veteran identification	Not used
Address	Veteran identification	Not used
Sex	Veteran identification	Not used
Employer	Veteran identification	Not used
Diagnosis Codes	Veteran insurance claim	Not used
Procedure Codes	Veteran insurance claim	Not used
Date Last Seen	Veteran identification	Not used
Admission Date/Visit Date	Veteran insurance claim	Not used

Discharge Date	Veteran insurance claim	Not used
Facility Name	Veteran insurance claim	Not used
Rated Disability/Eligibility	Veteran insurance claim	Not used
Treating/Discharge Specialty	Veteran insurance claim	Not used
Most Recent Date of Care	Veteran insurance claim	Not used
Medications	Veteran insurance claim	Not used
Provider Name	Veteran insurance claim	Not used
Subscriber identification number	Veteran insurance claim	Not used

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

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

Revenue Operations Payer Compliance Tool (ROPCT) is a **third-party** insurance account and payment data exploration tool. It provides scenario modeling and automatic calculation of insurance carrier agreements that compare actual reimbursements to expected payments and quantifies underpayments. ROPCT provides reports with various views, filters, customization, and search capabilities at the claim, VAMC, VISN, CPAC, and national level.

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

No data is being changed after it is extracted from VistA. The tool does not create or make available new or previously unutilized information about an individual.

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

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

Data at rest is protected via database encryption and role-based access control. Data in transit is protected via encrypted SSL connection for all remote access.

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

SSNs received database encryption.

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

Mitigations include the system being kept on the VA network, behind a VA firewall, with encryption of the databases, and the implementation of VA SSO, integrated. Access to PII is limited by the ROPCT to only those applications necessary for staff to perform their job, as determined by their management team and their job description. User roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles are determined by supervisors or higher. Users access is provided by CPAC OI&T following receipt of request from appropriate individuals.

2.4 PRIVACY IMPACT

ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

All users must complete a background check and receive authorization from the Dept. of VA to receive access to roles that expose PII.

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

Yes, procedures, controls, and responsibilities follow standard VA-defined processes and procedures for access to PII. Y

2.4c Does access require manager approval?

Yes

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

All systems storing PII have data access audited at a system and database level.

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

The Authorizing Officer is responsible for assuring 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*

The ROPCT application retains individual security information. The following data is stored on the ROPCT servers: Patient Name, Social Security Number, Date of Birth, Sex, Diagnosis Codes, Date Last Seen, Procedure Codes, Admission/Visit Date, Facility Name, Rated Disability/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications, Provider Name.

3.2 How long is information retained?

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

Prior to the implementation of the retention schedule referenced in the following question, ROPCT contains some data older than six years. This is expected to be addressed with the implementation of the retention schedule in development.

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

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

This question is related to privacy control DM-2, Data Retention and Disposal.

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

ROPCT maintains compliance with Records Control Schedule (RCS) 10-1, Chapter 4, Item 4000.1 a & 4000.1 b Financial Transaction Records related to procuring goods and services, paying bills, collecting debts, and accounting:

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

a. Official record held in the office of record. Temporary: destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. General Records Schedule (GRS) 1.1, Item 10 (Disposition Authority (AA)-GRS-2016-0001-0002)

b. All other copies temporary: destroy or delete when 6 years old, but longer retention is authorized if required for business use. GRS 1.1, Item 013 (DAA-GRS-2016-0001-0002)

3.4 What are the procedures for the elimination or transfer of SPI?

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

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.

Paper-based training materials are scrubbed from any PII information. When possible, a training system containing dummy account information is used for training. If a live system is required, it is operated behind a VA firewall in a secure environment.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The

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

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

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

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

Follow the format below:

Privacy Risk: Unnecessary retention of PII/SPI

Mitigation: Pending implementation of retention policy. Also, note that all information is stored on a secure server on VA premises. Mitigation is managed in accordance with Records Control Schedule (RCS) 10-1, Chapter 4, Item 4000.1a and 4000.1b Financial Transaction Records related to procuring goods and services, paying bills, collecting debt, and accounting:
a. Official record held in the office of record. Temporary: destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. General Records Schedule (GRS) 1.1, Item 10 (Disposition Authority (AA)-GRS-2016-0001-0002)
b. All other copies temporary: destroy or delete when 6 years old, but longer retention is authorized if required for business use. GRS 1.1, Item 013 (DAA-GRS-2016-0001-0002)

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***
VistA – Received	Fulfill auditing requirements	First Name, Last Name, SSN, DOB, Diagnosis Codes, Procedure Codes, Insurance Claim	Electronically transferred from FSC using File Transfer Protocols (FTP)
FSC – Received	Fulfill auditing requirements	First Name, Last Name, SSN, DOB, Diagnosis Codes, Procedure Codes, Insurance Claim	Electronically transferred from FSC using File Transfer Protocols (FTP)
VHA mobile Performance and Operational Web-enabled Reports (mPOWER)	Metric	Patient Name, SSN, DOB, Address, Sex, Employer, Diagnosis codes, Procedure codes, Date Last Seen, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications, Provider Name	Windows network sharing
Medispan	Fulfill auditing requirements	Pharmacy data including NDC, Drug Name, Drug Code, Manufacturers Labeler, Brand Name, Dosage	Electronically transferred. from Medispan using File Transfer Protocols (FTP)

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*
		Strength, Package Size, Package Units, Package Quantity, Package Code, Effective Date, End Date, Unit Price, Package Price, Price Code, AWP Indicator Code	
Cerner Oracle	Fulfill auditing requirements	Patient Name, SSN, DOB, Address, Sex, Employer, Diagnosis codes, Procedure codes, Date Last Seen, Admission Date/Visit Date, Discharge Date, Facility Name, Rated Disabilities/Eligibility, Treating/Discharge Specialty, Most Recent Date of Care, Insurance, Medications, Provider Name	Electronically transferred from Medispan using File Transfer Protocols (FTP)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The ROPCT collects both Personally Identifiable Information (PII) and limited other Sensitive Personal Information (SPI) such as financial information. Due to the sensitive nature of this information, there is a risk that access by an unauthorized person could result in serious personal, professional, or financial harm to the individual to whom the information pertains.

Mitigation: Mitigations include the system being kept on the VA network, behind a VA firewall, with encryption of the databases, and the implementation of VA SSO, integrated. Access to PII is

limited by the ROPCT to only those applications necessary for staff to perform their job, as determined by their management team and their job description. User roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles are determined by supervisors or higher. Users access is provided by CPAC OI&T following receipt of request from appropriate individuals.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the***	***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***	***List the method of transmission and the measures in place to secure data***

	specified program office or IT system		***sharing (can be more than one)***	
N/A				

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: None – No external information is shared or received with external organizations.

Mitigation: N/A

Section 6. Notice

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

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

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

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

Yes, notice is provided to Veterans at the time of enrollment on VA Form 10-10EZ.

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

A copy of VA Form 10-10EZ can be found online https://www.va.gov/vaforms/form_detail.asp?FormNo=10EZ.

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

The notice being provided is sufficient because our system is only used for internal data analysis and accounting by the VA and would not impact the Veteran.

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.

VHA Handbook 1605.1 'Privacy and Release Information' lists the rights of Veteran to request the VHA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. Veterans have the right to refuse to disclose their SSNs to the VHA.

The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)).

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

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

VHA Handbook 1605.1, Privacy and Release Information lists the rights of Veteran to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations.

6.4 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 System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of 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: The ROPCT systems collect both Personally Identifiable information (PII) and limited other Sensitive Personal Information (SPI) such as financial information. Due to the sensitive nature of this information; there is a risk that an access by an unauthorized person could result in a serious personal, professional or financial harm to the individual to whom the information pertains.

Mitigation: Contractor and VA employees are required to take Privacy, HIPAA, Rules of Behavior, and information security training annually. In addition, this PIA, which will be available online as required by the eGovernment Act of 2002, Pub.L. 107–347§208(b)(1)(B)(iii), serves to notify Veterans about the collection and storage of personal information.

Section 7. Access, Redress, and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?
These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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

VHA Handbook 1605.1: Privacy and Release Information states the rights of Veteran to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access to data must be delivered to, and reviewed by, the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their

designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The system is not exempt.

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

The system is a Privacy Act system.

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 authoritative source for the data is VistA. If data stored in the authoritative sources are erroneous, the OCC CPAC staff can take a note, but the Payer Compliance Tool application cannot be used to correct inaccurate or erroneous information stored in VistA. However, if a correction is requested by a Veteran, then such a request must be in writing and it must adequately describe the specific information that the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record or to the VBA. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. VHA Handbook 1605.1, Appendix D: Privacy and Release Information, Section 5 lists the rights of Veteran to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations.

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.

Office of Finance staff will notify the Veteran that they may change their information if the information presented is incorrect. VHA Handbook 1605.1, Appendix D: Privacy and Release Information, Section 8 states the rights of Veteran to amend their records by submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information that may be used as the written request requirement. This includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

If the Beneficiary discovers that incorrect information was provided during intake, they simply follow the same contact procedures in section 7-3 (also re-stated below), and state that the documentation they are now providing supersedes those previously provided.
If a Beneficiary discovers that incorrect information was provided during the intake process, the request must be in writing and adequately describe the specific information the Beneficiary believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:

Privacy Risk: There is a risk that incorrect information is accidently recorded in a Beneficiary's record. A Beneficiary may want to review the content of their record to check for data accuracy. The magnitude of harm associated with this risk to the VA would be low.

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

Section 8. Technical Access and Security

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

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

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

8.1a Describe the process by which an individual receives access to the system?
The supervisor/COR documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training. This documentation and monitoring are performed using the Talent Management System (TMS). Access to the system is granted to VA employees and contractors the supporting IT for the application after the supervisor/COR authorizes this access once requirements have been met. Only the IT system administrators authorized by VA IT will have the security role to modify the Payer Compliance Tool application. This PIA will not result in technology protocol changes, additional controls, nor single sign on, as per privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?
No users from other agencies 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.

Unique IDs and undisclosed passwords are required. Contractor support staff with administrative access rights that are granted through VA protocols that include single sign on capability. There are regular reviews of user access to evaluate whether users are active in the environment. If a user is not active, the account will be terminated. Only supervisors and above can submit account creation requests.

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.

VA contractors have access to the pre-production environments for development purposes. Contractors also have access to the live production system for maintenance activities. The following steps are required before contractors can gain access to the system:

- Contractors must take and pass training on privacy, HIPAA, information security, and government ethics and role-based training based on support role to the system.
- Contractors must have signed the Non-Disclosure Agreement (NDA) and VA Information Security Rules of Behavior (RoB).
- Contractors must have successfully completed VA contractor background security investigation as per the Position Designation Automated Tool (PDT).
- Once complete, a request is submitted for access. Before access is granted to the production environment: this request must be approved by the supervisor, information security officer and OIT.

VA owns the data that the RO Payer Compliance Tool application extracts from the source applications.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training.

Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees and contractors must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- Privacy and Info Security Awareness and Rules of Behavior
- Privacy and HIPAA Training

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 21 March 2022
3. *The Authorization Status:* ATO
4. *The Authorization Date:* 11 March 2021
5. *The Authorization Termination Date:10 March* 2024
6. *The Risk Review Completion Date:* 24 February 2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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.***

NA

Section 9 – Technology Usage

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

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

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

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

No, ROPCT does not use cloud technology. The software resides on a VA datacenter.

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

NA

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.

NA

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.

NA

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).

NA

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.

RHONDA SPRY-WOMACK

Digitally signed by RHONDA SPRY-WOMACK
Date: 2024.07.02 14:57:21 -05'00'

Privacy Officer, Rhonda Spry-Womack

MARK FARRIS

Digitally signed by MARK FARRIS
Date: 2024.07.02 16:05:36 -04'00'

Information System Security Officer, Mark Farris

LORI FRANKLIN

Digitally signed by LORI FRANKLIN
Date: 2024.07.03 07:26:20 -04'00'

Information System Owner, Lori Franklin

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).

- Privacy Act Information:

A copy of VA Form 10-10EZ can be found online at https://www.va.gov/vaforms/form_detail.asp?FormNo=10EZ.

"VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705,1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified from initial submission forward through a computer-matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the VHA Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law."

- VHA Direct 1605.1 - Privacy and Release of Information:

  A copy of VHA DIRECTIVE 1605.01 can be found online at https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=11388

HELPFUL LINKS:

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

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

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

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

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