Privacy Impact Assessment for the VA IT System called:

Portal for Electronic Third-Party Insurance Recovery (PETIR)

Veterans Health Administration (VHA)

eBusiness Solutions Office

eMASS ID #657

Date PIA submitted for review:

04 June 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Thomas Nsiah-Asare	Thomas.Nsiah-Asare@va.gov	5124605081
Information System Owner	Temperance Leister	Temperance.Leister@va.gov	4844326161

Abstract

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

Providing assistance for revenue collection efforts of VA Medical Centers the Portal for Electronic Third-party Insurance Recovery (PETIR) enables HIPAA mandated electronic data exchanges between VAMC's VistA systems and health plans/payers (with the assistance of healthcare and financial clearinghouses, which are part of the HIPAA Infrastructure). This national solution streamlines compliance with HIPAA by providing a single entity for managing the Electronic Data Interchange (EDI) IT infrastructure, processes, and expertise. PETIR uses commercial off the shelf (COTS) software to translate VistA into HIPAA transaction formats, route the data to appropriate external trading partners, accept incoming transactions from external trading partners, and translate health plan statuses and responses into formats acceptable to VistA before returning the information to VistA.

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?

Portal for Electronic Third-Party Insurance Recovery
Veterans Health Administration (VHA)
eBusiness Solutions

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

Electronic Data Interchange (EDI) - Lockbox (EPH), Insurance Identification and Verification eIV), Pharmacy Insurance Claims (PHR), Streamlines the management of multiple components, including simplification of documentation for security, disaster recovery, and privacy

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

VA Owned and VA Operated

2. Information Collection and Sharing

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

PETIR is used by about 100 VistA and Change HealthCare users. These product(s) are just a conduit of data between Change HealthCare and VistA

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

PII/PHI such as name, SSN, DOB, mailing address, zip code, phone number(s), insurance beneficiary information, current medications, previous medical records

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

Data in this system is shared with VistA and Change Health

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?

PETIR resides only in AITC

3. Legal Authority and SORN

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

Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Sections 501(a),1710, 1729 and Section 7304, Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36,39, 51,53, and 55 provide the legal authority for operating the PETIR system. Authority is from Title 38, United States Code, Section 5106 – Furnishing of information by other agencies. Public Law 99–272, Consolidated Omnibus Budget Reconciliation Act of 1985, enacted April 7, 1986 • 114VA10 - The Revenue Program Billings and Collection Records-VA o https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf

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?

SORN does not require revision or amendment

4. System Changes

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

No changes to business processes

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

No 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: None.

PII Mapping of Components (Servers/Database)

PETIR consists of two (2) key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by PETIR 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.

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

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
EIVP1	Yes	Yes	PII/PHI such as name, DOB, mailing address, zip code, phone number(s), health insurance beneficiary information, current medications, previous medical records.	VA health insurance eligibility requests and health plan responses between VAMC VistA systems and external trading partners, Medicare Remittance Advice, exchanges third-party health care claims and status messages, outpatient pharmacy claims and health plan responses, processing of third-party healthcare claims and health plan payments and provide Electronic Explanation of Benefits (EEOB).	The data center hosting these servers monitors all internet gateways; employs network and host-based intrusion detection; collects, reviews, and retains server event logs in a secure database; employs antivirus protection and applies operating system patches; develops and maintains configuration controls on all servers.
EPHRAP1	Yes	Yes	PII/PHI such as name,	VA health insurance	The datacenter

			DOB, mailing address, zip code, phone number(s), health insurance beneficiary information, current medications. previous medical records.	eligibility requests and health plan responses between VAMC VistA systems and external trading partners, Medicare Remittance Advice, exchanges, and third-party health care claims.	hosting these servers monitors all internet gateways; employs network and host-based intrusion detection; collects, reviews, and retains server event logs.

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?

VistA and Change Healthcare

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

Information from VistA and Change HealthCare are necessary to process medical prescriptions for the Veterans

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

- Veterans Health Information Systems and Technology Architecture (VistA) – derived from various sources including the Veteran, care providers and other systems connected to VistA
- Optum
- PNC Bank
- Department of Health and Human Services (HHS)
- Centers for Medicare and Medicaid (CMS)
- PNT Data Corporation

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

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

Information is provided via electronic transmission.

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?
Information is not collected via form under the Paperwork Reduction Act

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.

Data can be checked for completeness by system audits, manual verifications, and annual questionnaires through automated Veteran letters

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?
The PETIR system assumes that information was checked for accuracy when it was first entered the source systems. Data can be checked for completeness by system audits, manual verifications and annual questionnaires through automated Veteran letters. PETIR components check the information input for reasonableness, completeness, and validity. Edits exist in the process to validate the data sent from VistA. For example, PETIR edits the data to ensure that every line item on a claim has a charged amount. For specific details on how eBusiness processes, refer to the FSC eBusiness Solutions team procedures documentation for eClaims, eMRA, eIV, ePayments, and the ePharmacy components.

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

Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Sections 501(a), 1710, 1729 and Section 7304(a), Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36,

39, 51,53, and 55 provide the legal authority for operating the PETIR system. Authority is from Title 38, United States Code, Section 5106 – Furnishing of information by other agencies.
Public Law 99–272, Consolidated Omnibus Budget Reconciliation Act of 1985, enacted April 7, 1986
Authority under 114VA10 - The Revenue Program Billings and Collection Records-VA https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf: Title 38, United States Code (U.S.C.), sections 1710 and 1729.

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: PETIR collects data to support the mission of the VA supporting health care provided to Veterans if the form of revenue collection and billing of services to third party insurance companies. The PETIR system collects stores and transmits a large amount of PHI/PII. Therefore, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, or misused, serious personal/professional or financial harm may result for the individuals affected. Additionally, the compromise of this information would constitute a breach of confidence with the Veterans served by VHA.

Mitigation: PETIR enables HIPAA-mandated electronic data exchanges between VAMCs VistA systems and health plans/payers (with the assistance of healthcare and financial clearinghouses, which are part of the HIPAA infrastructure). PETIR components rely on the underlying enterprise infrastructure for file system protection. Application data is protected by user access permissions. Data confidentiality and integrity is also ensured via administrative, technical, and

physical controls. Physical access to Infrastructure Operations (IO) servers is restricted to authorized personnel in a data center at a facility with 24-hour security. Network access to servers is managed through firewalls. Access via the network requires authentication for both the application and servers. Employing user logon access controls, strict VA and Office of Inspector General (OIG) policies with training, and a physically secure facility are all controls that aid in keeping the data confidential. VA 6500 implementation of this control states that database management systems used in VA will be encrypted using FIPS 140-2 (or its successor) validated encryption. The encryption of database management systems is currently implemented within FSC. PETIR users submit an access request application using a VA Form 9957. To ensure accountability, all user accounts on VA information systems must be individualized. Use of individual passwords is mandated. User Identification (user ID) and associated passwords are personal to the individual owner and must be chosen and protected with care. Only the user to whom the passwords are assigned will use the passwords. All passwords are considered sensitive information and must be treated as such. They may not be shared with anyone. Users are accountable for actions performed with their user ID and will be held liable for actions determined to be intentionally malicious, grossly negligent, or illegal. A user may not log on to any Infrastructure Operations (IO) system or network unless they are properly registered in and authorized to use that system or network.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Identification of Patient	Identification of Patient
Date of Birth	Identification of Patient	Identification of Patient
Personal Mailing Address	Identification of Patient	Communication with Patient
Personal Phone Number(s)	Identification of Patient	Communication with Patient
Personal Email Address	Identification of Patient	Communication with Patient
Health Insurance Beneficiary Information	Claims/Eligibility	Claims/Eligibility
Current Mediation(s)	Claims/Eligibility	Claims/Eligibility
Previous Medical Record(s)	Claims/Eligibility	Claims/Eligibility

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?
PETIR uses COTS software to translate VistA data into HIPAA transaction formats, route the data to appropriate external trading partners, accept incoming transactions from external trading partners, and translate health plan statuses and responses into formats acceptable to VistA before returning the information to VistA. This information system is used during business hours primarily for real time data exchanges and internal reporting, and off-peak hours for scheduled batch data exchanges.

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.

PETIR uses COTS software to translate VistA data into HIPAA transaction formats, route the data to appropriate external trading partners, accept incoming transactions from external trading partners, and translate health plan statuses and responses into formats acceptable to VistA before returning the information to VistA. This information system is used during business hours primarily for real time data exchanges and internal reporting, and off-peak hours for scheduled batch data exchanges.

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?
Connectivity with External Trading Partners is secured using Site-to-Site VPN tunnel managed by VA NOC. The message exchange is encrypted and uses HTTPS protocol.

At Rest, the data resides on systems/databases within the VA LAN/WAN that reside behind the VA firewall. ACL is regularly reviewed, and all access is governed through Elevated Privilege framework.

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

Additional protections in place are that the data payload is encrypted besides the message itself (HTTPS), when it's in transit to the external trading partner.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
The communication with Trading Partner is HTTPS using 2-way SSL.
Transport-level security –
- *Site-to-Site VPN tunnels going through TICGATEWAY managed by NOC*

- *SSL Connection using RSA256 Certs*
- *Support for specific ciphers ONLY*

Message Level security –

- *Digitally sign payload using RSA-SHA2*

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?

The official system of records notice (SORN) for these can be found on-line at http://www.oprm.va.gov/privacy/systems_of_records.aspx
Following are the SORNS and data:

- 114VA10 - The Revenue Program Billings and Collection Records-VA
- https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf

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

The security for the PETIR application covers 32 security controls with regards to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition. system and communications protection; and system and information integrity. The PETIR application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how Veterans' information is used, stored, and protected.

2.4c Does access require manager approval?

Yes

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

<<PII data is not accessible.>>

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

System Administrators

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
• DOB
• Personal Mailing Address
• Personal Phone Number(s)
• Personal Email Address
• Health Insurance Beneficiary Information
• Current Medications
• Previous Medical Records

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.*

In accordance with the SORN, longer retention is authorized. The sorn follows the requirements of RCS 10–1 Chapter 4 Item 4000.1 a & b. 4000.1 Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting. a. Official record held in the office of record. Temporary; destroy six (6) years after final payment or cancellation, but longer retention is authorized if required for business use. (GRS 1.1, Item 010) (DAA–GRS–2016–0001–0002) b. All Other copies Temporary; destroy or delete when six (6) years old, but longer retention is authorized if required for business use. (GRS 1.1 item 013) (DAA–GRS–2016– 0001–0002).

• RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

• National Archives and Record Administration: www.nara.gov

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

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

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

• RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

• National Archives and Record Administration: www.nara.gov

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

- RCS 10-1 and RCS VB are approved by NARA
- Retention period for HIPAA transactions specified by the Department of Health and Human
- Services (HHS)
- Centers for Medicare and Medicaid Services (CMS)

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.

Electronic media sanitization when the records are authorized for destruction (or upon system decommission) will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization.

Disposition of Printed Data:
Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks, and disposed of properly by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

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.

N/A, no PII is used for research, testing, or training. No PII is maintained in other than the PETIR production 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: There is a risk that the information maintained by PETIR could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention PETIR adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, "Management of Data Breaches Involving Sensitive Personal Information (SPI)" contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

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***
VA Medical Centers	Centers provide input data for PETIR system eClaims - Healthcare Claims from 127 VA field facilities in proprietary VistA format eIV- determination of eligibility for claimed insurance (Verification)	Name DOB SSN Mailing Address Zip code Phone Number(s) Health Insurance Beneficiary Information Current Medications Previous Medical Records Personal Email Address	Secure electronic data exchange Secure FTP (SFTP) transfer twice daily HL7 message exchange using TCP/IP protocol

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*
Financial Services Center (FSC)	FSC provides input data for PETIR system eMRA – Medicare claims ePayments - electronic healthcare payment and remittance advices ePharmacy – third party pharmacy claim data EPHRA – Electronic EOB data	• Name • DOB • SSN • Mailing Address • Zip Code • Phone Number(s) • Health Insurance • Beneficiary Information • Current Medications • Previous Medical Records	Secure electronic data exchange

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: PETIR contains a large amount of PHI and PII, which is necessary to process medical insurance claims and payments. The compromise of this information would constitute a breach of confidence with the Veterans served by VHA.

Mitigation: Access control for PETIR is limited for PII and PHI. The data already exists in the other systems without PETIR, and the electronic transfers of information are secure. All access is done through secure internal VA networks. Only selected users have access to the PETIR data. All users sign adherence to VA's strict privacy and security controls and must be current on VA Privacy and Information Security Awareness Rules of Behavior training. A properly executed VA form 9957 is required for access to PETIR as described in section 1.7.

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 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***
PNC Bank Enterprise File Transfer (EFX) Platform is the	ePayments - electronic healthcare payment and remittance advices.	• Name • DOB • SSN • Mailing Address • Zip Code • Phone Number(s)	PETIR-PNC Bank ISAMOU	Secure electronic data exchange. Site-to-Site VPN

System Name for PNC Bank	Functions as the VA 3rd Party Lockbox bank and accepts standard transactions from payers on behalf of the VA. PNC sends VA payment and Remittance advice information, and VA sends acknowledgments back to PNC.	• Health Insurance • Beneficiary Information • Current Medications • Previous Medical Records		
TransUnion Healthcare LLC (formerly MedData LLC) Healthcare EDI Transaction System is also the System name for TransUnion Healthcare LLC PNT Data Corporation	Bidirectional transfer to deliver health care eligibility inquiries to TransUnion for subsequent transport to health plans and to return health plan responses to the VA	• Name • DOB • SSN • Mailing Address • Zip Code • Phone Number(s) • Health Insurance • Beneficiary Information • Current Medications • Previous Medical Records	PETIR-TransUnion ISAMOU	Secure electronic data exchange. Site-to-Site VPN connection
Centers for Medicare and Medicaid Services (CMS)	VA exchanges Medicare Eligibility transactions	• Name • DOB • SSN • Mailing Address • Zip Code • Phone Number(s) • Health Insurance • Beneficiary Information • Current Medications • Previous Medical Records	PETIR-CMS_ HETS TPA-Trading Partner Agreement	Direct Connect
Optum	To deliver VHA electronic healthcare transactions to	• Name • DOB • SSN • Mailing Address	ISAMOU	Site to Site (S2S VPN)

	Optum for subsequent delivery to other covered entities, including health plans, and to deliver covered entities and Optum responses back to the VA.	• Zip Code • Phone Number(s) • Health Insurance • Beneficiary Information • Current Medications • Previous Medical Records		
Optum	To deliver VHA electronic healthcare transactions to Optum for subsequent delivery to other covered entities, including health plans, and to deliver covered entities and Optum responses back to the VA.	• Name • DOB • SSN • Mailing Address • Zip Code • Phone Number(s) • Health Insurance • Beneficiary Information • Current Medications • Previous Medical Records	ISAMOU	Cloud Service Provider/S2S (CSP/S2

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: There is a risk that information may be shared with an unauthorized program, system, or individual.

Mitigation: The System Interconnect Agreement/Memorandum of Understandings are in place. These documents define the terms and conditions for sharing the data to and from the VA. Safeguards are implemented to ensure data is not sent to the wrong organization, program, or system. VA
employees, contractors, and business partners take security and privacy training and awareness and are required to report suspicious activity. Use of secure passwords, access for need-to-know basis, encryption, and access authorization are all measures that are utilized within the facilities. In addition, the systems that receive the data from FSC are covered entities under the HIPAA privacy rules (see 45 CFS part 160 and subparts A and E of Part 164). These rules established a national privacy standard for medical records across the healthcare industry including restricting access to the data. By limiting the scope of data exchanges to only HIPAA covered entities; VA can reasonably expect that the receiving system has implemented safeguards to protect the information in compliance with the existing federal regulations.

Section 6. Notice

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

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

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

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

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
The System of Record Notice (SORN) “114VA10 - The Revenue Program Billings and Collection Records-VA.
o https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf

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.

This Privacy Impact Assessment (PIA) also serves as notice of the PITC Virtual VA system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

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.

No information is directly collected from the Veteran by PETIR so there is no opportunity to decline to provide information.

A Veteran may have the opportunity or notice of the right to decline to provide information to the source systems (such as VistA) that collects the information from the Veteran. By declining to supply information to the source system, the Veteran would also be declining the information to the PETIR system and other downstream applications.

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.

Any right to consent to uses of the information would be handled by the source systems that collect the information from the Veteran and feed PETIR with information.

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

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

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

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

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

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by PETIR.

Mitigation: Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1. MOU/ISA documents and business associate agreements along with the HIPAA Eligibility Transaction System (HETS) Trading Partner Agreement with CMS, provide a binding agreement and procedures to protect the data transferred.

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.***

PETIR is covered by SORN 114VA10 - The Revenue Program Billings and Collection Records-VA https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf which specifies access procedures as: Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they were treated.

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 as it is covered by the SORN 114VA10 as stated above.

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?

PETIR is covered by SORN 114VA10 - The Revenue Program Billings and Collection Records-VA https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1,

state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is 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. PETIR is covered by SORN 114VA10 - The Revenue Program Billings and Collection Records-VA https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf which specifies access procedures as: Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they were treated.

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.

In addition to the written and published SORN as listed above, individuals seeking information regarding access to and contesting of records in this system may write or call the VHA Director of National Data Systems (19F4), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at 512–326–6780.

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.

Formal redress is provided thru the source documents. PETIR is covered by SORN 114VA10 - The Revenue Program Billings and Collection Records-VA https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf which specifies

access procedures as: Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they were treated.

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 members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information that is collected and maintained regarding this system.

Mitigation: The risk of incorrect information in an individual's records is mitigated by authenticating information when possible. The process for access, correcting and contesting information is identified in the System of Records Notices and the Notice of Privacy Practices discusses the process for requesting an amendment to one's records. This PIA also serves to notify individuals of their rights to access, correct and contest the information that is maintained.

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?

Access to the mainframe component of PETIR is granted by submitting a VA Form 9957 Access Form with appropriate functional task codes to Program staff, who grant system access.

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?
PETIR systems cannot be accessed and is not accessible from outside agencies or entities.

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.

Standard system administrator roles only (PETIR Linux Administrator, Database Administrator and Middleware Administrator)

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.

Contractors can be granted access to PETIR if their VA manager, COR and the Information System Security Officer (ISSO) approve. They are required to follow the same procedures VA employees do for access, which is to submit a 9957 form. In addition, in accordance with the contract between the contractor and the government, all contractors with access to PETIR information are required to meet VA contractor security requirements.

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 that will be accessing information systems must read and acknowledge their receipt

and acceptance of the VA 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 which all personnel must complete via the VA's Talent Management System (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 is obtained via electronic acknowledgment and is tracked through the TMS system. VA users with access to protected health information must complete mandatory HIPAA Privacy training annually in TMS.

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

8.4a If Yes, provide:

1. *The Security Plan Status:*14-Nov-2022
2. *The System Security Plan Status Date:*14-Nov.2022
3. *The Authorization Status:* Current
4. *The Authorization Date:* 28-Feb-2022
5. *The Authorization Termination Date:* 01-Aug-2024
6. *The Risk Review Completion Date:* 18-Feb-2022

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.***

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.

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.*

There is no agreement between the VA and the Cloud Service Provider as PETIR does not operate in the Cloud.

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.

PETIR does not operate in the Cloud.

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.

PETIR does not operate in the Cloud.

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).

PETIR does not utilize the Robotic Automation Process.

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

ID	Privacy Controls
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.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.09.03 13:36:38 -04'00'

Privacy Officer, Nancy Katz-Johnson

THOMAS NSIAH-ASARE

Digitally signed by THOMAS NSIAH-ASARE
Date: 2024.09.05 09:20:09 -05'00'

Information System Security Officer, Thomas Nsiah-Asare

TEMPERANCE LEISTER

Digitally signed by TEMPERANCE LEISTER
Date: 2024.09.05 08:13:58 -05'00'

Information System Owner, Temperance Leister

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).

The System of Record Notice (SORN) “114VA10 - The Revenue Program Billings and Collection Records-VA.
o https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf

Privacy Impact Assessment (PIA)

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 1605.04