Privacy Impact Assessment for the VA IT System called:

Program Integrity Tool (PIT)

Veterans Health Administration (VHA)

Office of Integrated Veteran Care

eMASS ID # 1239

Date PIA submitted for review:

5/23/2024

System Contacts:

System Contacts

Title	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Eric Bailey	eric.bailey3@va.gov	973-676-1000 x202494
Information System Owner	Tony Sines	tony.sines@va.gov	316-249-8510
Data/Business/Information Owner[2]	Jennifer Adams	Jennifer.Adams26@va.gov	615-355-1539

Abstract

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

Program Integrity Tool (PIT) interfaces to VHA Office of Integrated Veteran Care databases, feeding a repository with a claim scoring tool that scores incoming claims for risk of fraud, waste and abuse.

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?

Program Integrity Tool (PIT) / VHA Office of Integrity and Compliance

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 application is part of Major Initiative (MI)-15 Health Care Efficiency and interfaces to VHA Office of Integrated Veteran Care databases, feeding a repository with a claim scoring tool that scores incoming claims for risk of fraud, waste and abuse.

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?

There are over 50,000 claim individuals that have stored information.

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

The application repository collects claims and patient clinical data in order to score incoming claims for risk of fraud, waste and abuse.

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

Program Integrity Tool (PIT) is a Microsoft Azure application hosted at VAEC, part of Major Initiative (MI)-15 Health Care Efficiency. The application will interface to Veterans Health Administration (VHA) Office of Integrated Veteran Care (IVC) databases, feeding a repository with a claim scoring tool that will score incoming claims for risk of fraud, waste and abuse. PIT is comprised of multiple components. The data repository is at the core of the Program Integrity Tool (PIT) system, it receives data feeds

from other VA claim processing systems including Community Care Non-Network Care Provider Portal (CCNNC (eCAMS)), Claims Processing and Eligibility (CP&E), Veterans Choice System, and Corporate Data Warehouse (CDW); each source system providing data to a central drop zone. 1. A Central Enterprise Repository that will be fed from multiple claims systems to provide claims and patient clinical data through Extract Transform Load (ETL) Tools. 2. A Fraud/Waste/Abuse (FWA) or claims scoring to detect and deter fraud/waste and abuse on a post-payment basis. 3. The Dashboard and Reporting application that will accommodate end-user browsing and analysis, standardized reports, ad hoc queries and reports and business intelligence extractions which we anticipate will be used to manipulate dimensional presentation of data.

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

No. PIT is located in VA Enterprise Cloud (VAEC) Azure.

3. Legal Authority and SORN

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

SORN: 23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015),
https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf
Legal Authority: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.
SORN: 172VA10, VHA Corporate Data Warehouse-VA (12/22/2021)
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf
Legal Authority: Title 38, United States Code, Section 501.

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 SORNs will require amendment due to being over 6 years old.

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 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:

- Veteran Service-Connected Status and Conditions
- Diagnosis Codes
- Pharmacy Information
- Previous Medical Records
- Procedure Codes
- Provider Information
- Insurance Information

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

- Payment Information
- Claim Information

PII Mapping of Components (Servers/Database)

Program Integrity Tool (PCI) (Cloud) consists of 4 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Program Integrity Tool (PCI) (Cloud) 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
Liberty, Tomcat, WebSphere	Yes	No	Beneficiary Numbers, Account Numbers, Previous Medical Records, Veteran Service-Connected Status and Conditions	Provides post-payment Fee Basis claims data to PIT for evaluation of fraud, waste, and abuse	Secure data transfer via direct ODBC connection behind the VA firewall with subsequent, secure Extract Transform Load (ETL) integration of data into PIT
PITEDR	Yes	No	Address, Date of Birth, Diagnosis Codes, Insurance Information, Address, Name,	Provides post-payment Fee Basis claims data to PIT for evaluation of fraud, waste, and abuse	Secure data transfer via direct ODBC connection behind the VA firewall with subsequent, secure

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
			Pharmacy Information, Phone Number, Procedure Codes, Provider Information, SSN		Extract Transform Load (ETL) integration of data into PIT
Internal PIT Dev Team	Yes	No	Name, SSN, Date of Birth, Address, Health Insurance Beneficiary Numbers Account Numbers, Previous Medical Records, Veteran Service-Connected Status and Conditions	Provides post-payment Fee Basis claims data to PIT for evaluation of fraud, waste, and abuse	Secure data transfer via direct ODBC connection behind the VA firewall with subsequent, secure Extract Transform Load (ETL) integration of data into PIT
FAMSDMSQ	Yes	No	Name, SSN, DOB, Address, Phone Number, Insurance Information, Provider Information, Pharmacy Information, Procedure Codes,	Provides post-payment Fee Basis claims data to PIT for evaluation of fraud, waste, and abuse	Secure data transfer via direct ODBC connection behind the VA firewall with subsequent, secure Extract Transform Load (ETL) integration

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
			Diagnosis Codes		of data into PIT

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?

PIT gathers information from the following systems: Community Care Non-Network Care Provider Portal (CCNNC (eCAMS)), Corporate Data Warehouse (CDW), Community Care Reimbursement System (CCRS), Veterans Choice system for the evaluation of fraud, waste, and abuse.

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.

All information is gathered from internal VHA sources for the evaluation of fraud, waste, and abuse.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
The Dashboard and Reporting application accommodates end-user browsing and analysis, standardized reports, ad hoc queries and reports and business intelligence extractions.

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?

PIT collects Sensitive Personal Information (SPI) to include Personal Identifiable Information (PII) and Protected Health Information (PHI) via secure electronic transfer from other internal VA systems listed in section 1.2.

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 on a form.

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.

As information for the PIT system is imported from existing VA systems, the accuracy is verified by the original source systems prior to transmitting the data to the PIT system.

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 PIT system does not check for accuracy by accessing a commercial aggregator of information. Information for the PIT system is verified for accuracy and imported from existing VA systems.

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

SORN: 23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015),
https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf
Legal Authority: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.
SORN: 172VA10, VHA Corporate Data Warehouse-VA (12/22/2021)
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf.
Legal Authority: Title 38, United States Code, Section 501.

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: PIT collects Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and aid the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA can better protect the individual's information.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Veteran identification	Data Transmission

PII/PHI Data Element	Internal Use	External Use
Social Security Number	Veteran identification	Data Transmission
Date of Birth	Veteran identification	Data Transmission
Address	Corresponding with Veteran	Data Transmission
Health Insurance Beneficiary Numbers Account Numbers	Claims verification	Data Transmission
Medical Records	Claims verification	Data Transmission
Veteran Service-Connected Status and Conditions	Claims verification	Data Transmission
Diagnosis Codes	Claims verification	Not used
Pharmacy Information	Claims verification	Not used
Phone Number	Claims verification	Not used
Previous Medical Records	Claims verification	Data Transmission
Procedure Codes	Claims verification	Not used
Provider Information	Claims verification	Not used
Insurance Information	Claims verification	Not used
Payment Information	Claims verification	Not used
Claim Information	Claims verification	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?

The Fraud/Waste/Abuse (FWA) or claims scoring segments of the PIT application analyze data to detect and deter fraud/waste and abuse of claims on a post-payment basis. Claims scored or flagged for potential FWA will be forwarded to the proper authority for manual adjudications and possibly forwarded for criminal investigations.

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

The system does not create or make available new or previously 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 Segmentation and encryption of data at rest: Personal Identification Verification is Enabled and Enforced. The NSOC is responsible for establishing and maintaining cryptographic keys used within VA and can retrieve those that have been forgotten or lost DCO information systems employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. DCO facilities participate in VA Public Key Infrastructure (PKI) program developed by VAs Office of Information and Technology (OI&T). There are automated mechanisms with supporting manual procedures for cryptographic key establishment and key management. VA has established processes for the delivery and use of both "soft" and "hard" certificates and the use of Personnel Identity Verification (PIV) cards for purposes of authentication, encryption, and decryption.

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

Data Segmentation and encryption of data at rest: Personal Identification Verification is Enabled and Enforced. The NSOC is responsible for establishing and maintaining cryptographic keys used within VA and can retrieve those that have been forgotten or lost DCO information systems employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. DCO facilities participate in VA Public Key Infrastructure (PKI) program developed by VAs Office of Information and Technology (OI&T). There are automated mechanisms with supporting manual procedures for cryptographic key establishment and key management. VA has established processes for the delivery and use of both "soft" and "hard" certificates and the use of Personnel Identity Verification (PIV) cards for purposes of authentication, encryption, and decryption.

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

Data Segmentation and encryption of data at rest: Personal Identification Verification is Enabled and Enforced. The NSOC is responsible for establishing and maintaining cryptographic keys used within VA and can retrieve those that have been forgotten or lost DCO information systems employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management. DCO facilities participate in VA Public Key Infrastructure (PKI) program developed by VAs Office of Information and Technology (OI&T). There are automated mechanisms with supporting manual procedures for cryptographic key establishment and key management. VA has established processes for the delivery and use of both "soft" and "hard" certificates and the use of Personnel Identity Verification (PIV) cards for purposes of authentication, encryption, and decryption.

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?

PIT limits access to PII to only those staff that is deemed necessary to do their jobs as determined by their management team and job description. Supervisors request access for staff by role.

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

Yes, procedures are in place regarding access. PIT follows standard VA Policy and procedures when granting access to its system. Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. VA OIT implements data protection assurances on all databases where patient insurance information is stored. Limited system access is granted by VA OIT to ensure only those with need to know have access to any patient related data. VA OIT periodically audits user accounts and removes access to those who no longer need access or have not used granted access in the previous audit period.

2.4c Does access require manager approval?

Yes. Manager approval is required through ePAS requests.

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

Access is monitored through audit logging .

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

VAEC and PIT 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, Social Security Number, Date of Birth. Address, Health Insurance Beneficiary Numbers Account Numbers, Previous Medical Records, Veteran Service-Connected Status and Conditions, Diagnosis Codes, Pharmacy Information, Phone Number, Procedure Codes, Provider Information, Insurance Information, Payment Information, Claim Information

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.*

The various systems supplying data to PIT have varied retention schedules outlined below: 23VA10NB3: Non-VA Care (Fee) Records-VA: Paper and electronic documents at the authorizing healthcare facility related to authorizing the Non-VA Care (fee) and the services authorized, billed and paid for are maintained at healthcare facilities for a minimum of three years after the last episode of care. After the third year of inactivity the paper records are transferred to a records facility for seventy-two (72) more years of storage. Automated storage media, imaged Non-VA Care (fee) claims, and other paper documents that are included in this system of records and not maintained in ‘‘Patient Medical Records—VA’’ (24VA10A7) are retained and disposed of in accordance with disposition authority approved by the Archivist of the United States. VHA Corporate Data Warehouses— VA’’ (172VA10). Records are maintained and disposed of in accordance with General Records Schedule 20, item 4, which provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes.

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

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

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

Yes

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

Record Control Schedule (RCS) 10–1 item (http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf). 1260.1 Care in Community, Care in the Community, Health and Medical Care Program records include but not limited to: Veteran and beneficiary claim and administrative records

related to receiving health care services at VA expense outside VA facilities. A typical record file includes eligibility information, claim forms, medical records in support of claims and data concerning health care providers, services provided, amounts claimed and paid for health care services.

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 OIT-OIS SOP MP-6 Electronic Medial Sanitization. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1, Electronic Media Sanitization. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. 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 (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371, Destruction of Temporary Paper Records. 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.

PIT uses test data in a testing environment for testing the system. VA Handbook 6500 mandates that Systems under development should not process “live data” or do any real processing in which true business decisions will be based. Test data that is de-identified should be used to test systems and develop systems that have not yet undergone security A&A. Furthermore, systems that are in development (pilot, proof-of-concept, or prototype) should not be attached to VA networks without first being assessed and authorized. Additionally, VA wide Directive 6511 describes the responsibilities, requirements and procedures for eliminating PII or information exempt from release under FOIA from presentations that may be seen by non-VA parties. This Directive includes guidance for conducting privacy reviews of presentations, and the criteria for when presenters must self-certify that their presentations are devoid of PII or information exempt from release under FOIA.

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 PIT 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, the PIT 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 Breaches involving sensitive personal information, which 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***
Veterans Health Administration (VHA) Community Care Non-Network Care Provider Portal (CCNNC (eCAMS))	Provides post-payment Fee Basis claims data to PIT for evaluation of fraud, waste, and abuse.	Name, DOB, SSN, Insurance Information, Address, Phone Number, Provider Information, Medical Records	Secure data transfer via Windows file share using a drop zone behind the VA firewall, with subsequent, secure Extract Transform Load (ETL) integration of data into PIT.
Veterans Health Administration (VHA) Community Care Referral and Authorization CCRA (HSRM)	Provides post-payment Fee Basis claims data to PIT for evaluation of fraud, waste, and abuse.	Insurance Information, Provider Information	Transmitted via SFTP
Veterans Health Administration (VHA) Corporate Data warehouse (CDW)	Provides post-payment Fee Basis claims data to PIT for data analysis/reporting.	Name, DOB, SSN, Insurance Information, Address, Phone Number, Provider Information, Medical Records	Secure data transfer via direct ODBC connection behind the VA firewall, with subsequent, secure Extract Transform Load (ETL) integration of data into PIT

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*
Veterans Health Administration (VHA) Claims Processing & Eligibility System (CP&E)	Provides post-payment Fee Basis claims data to PIT for evaluation of fraud, waste, and abuse.	Name, DOB, SSN, Insurance Information, Address, Phone Number, Provider Information, Payment Information	Transmitted via Common Internet File System (CIFS) on Community Care File Transfer System (MoveIT)
Veterans Health Administration (VHA) Community Care Reimbursement System (CCRS)	Provides post-payment Fee Basis claims data to PIT for data analysis/reporting.	Name, DOB, SSN, Insurance Information, Address, Phone Number, Provider Information, Medical Records	Secure data transfer via direct ODBC connection behind the VA firewall, with subsequent, secure Extract Transform Load (ETL) integration of data into PIT.
Veterans Health Administration (VHA) Veterans Choice System	Provides post-payment Fee Basis claims data to PIT for evaluation of fraud, waste, and abuse.	Name, DOB, SSN, Insurance Information, Address, Phone Number, Provider Information, Medical Records	Secure data transfer via direct ODBC connection behind the VA firewall, with subsequent, secure Extract Transform Load (ETL) integration of data into PIT.
Veterans Health Administration Office of Integrated Veteran Care Payer Electronic Data Interchange Transactions Applications Suite (Payer EDI TAS)	Provides post-payment Fee Basis claims data to PIT for evaluation of fraud, waste, and abuse.	Name, DOB, SSN, Address, Phone Number, Health Insurance Beneficiary Numbers Account Numbers, Previous Medical Records, Veteran Service-Connected Status and Conditions, Diagnosis Codes, Pharmacy Information, Procedure Codes, Insurance Information, Provider Information, Payment Information, Claim Information	Transmitted via Azure Copy (AzCopy)

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*
Veterans Health Administration (VHA) Provider Profile Management System (PPMS)	Directory of authorized providers within the VA Network	DOB, SSN	Manual upload of a **.CSV** file to the PPMS SharePoint drop zone.

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 privacy risk associated with maintaining PII is that sharing data within the Department of Veterans Affairs could happen and that the data may be disclosed to individuals who do not require access which heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by PIT personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within. Access control occurs through the use of VA form 9957 with the end user's manager's approval and authorized by the appropriate System Manager of Record (SMR) or System Manager of Record Designee (SMRD).

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***
National Plan and Provider Enumeration (NPPES) Centers for Medicare and Medicaid Services (CMS)	Data Transmission	Name, Social Security Number, Date of Birth, Address, Diagnosis codes, Health Insurance Beneficiary Numbers, Account Numbers, Previous Medical Records, Veteran Service-Connected Status and Conditions	MOU/ISA	Encrypted SSL/HTTPS
Health and Human Services Office of Inspector General (HHS OIG)	List of Excluded Individuals and Entities (LEIE) file	List of Excluded Individuals and Entities (LEIE) file	MOU	Manual download from oig.hhs.gov

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 Memorandum of Understanding / Interconnection Security Agreement (MOU/ISA) is 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.

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.

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.
This Privacy Impact Assessment (PIA) also serves as notice 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."
Notice is also provided in the Federal Register with the publication of the SORN.

23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015).
172VA10, VHA Corporate Data Warehouse-VA (12/22/2021)
Privacy Act System of Records Notices (SORNs) site:
https://department.va.gov/privacy/system-of-records-notices/

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

Notice was provided as indicated above in question 6.1a.

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 is the only form of notice, as information is not collected directly from an individual. PII/PHI is collected by a commercial non-VA provider at the point of service. Information is collected from a non-government source and sent either from the Third-Party Administrators (TPA) or directly from a non-VA provider, so there is no opt-out or explanation of government use.

SORNs
23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015).
172VA10, VHA Corporate Data Warehouse-VA (12/22/2021)
Privacy Act System of Records Notices (SORNs) site:
https://department.va.gov/privacy/system-of-records-notices/

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them

from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with VHA.

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.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

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: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records. The NOPP is also available at all VHA medical centers from the facility Privacy Officer.

The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

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.***

The data repository is at the core of the Program Integrity Tool (PIT) system, receives data feeds from other VA claim processing systems including Community Care Non-Network Care Provider Portal (CCNNC (eCAMS)), Claims Processing and Eligibility (CP&E), Veterans Choice System, and Corporate Data Warehouse (CDW); The system falls under SORN 23VA10NB3 SYSTEM NAME: Non-VA Care (Fee) Records-VA which describes record access and contesting procedures: RECORD ACCESS PROCEDURE: Individuals seeking information regarding access to health records and/ or contesting health l records may write, call or visit the VA facility where medical care was last authorized or provided. Individuals seeking information regarding access to claims and/or billing records will write to the VHA Chief Business Office Purchased Care, Privacy Office, PO BOX 469060, Denver, CO. All Requests for records about

another person are required to provide a Request for an Authorization to Release Medical Records or Health Information signed by the record subject by using form VA Form 10–5345.

SORN ‘‘VHA Corporate Data Warehouses— VA’’ (172VA10) lists record access and contesting: Individuals seeking information regarding access to and contesting of records contained in this system of records may write to the Director of National Data Systems (105HIG), Austin Information Technology Center, 1615 Woodward Street, Austin, TX 78772. Inquiries should include the person’s full name, Social Security number, location and dates of employment or location and dates of treatment, and their return address.

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

Not Applicable. The system is not exempt from the access provisions of the Privacy Act.

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

Not Applicable. 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.

23VA10NB3 SYSTEM NAME: Non-VA Care (Fee) Records-VA describes record access and contesting procedures: RECORD ACCESS PROCEDURE: Individuals seeking information regarding access to health records and/ or contesting health l records may write, call or visit the VA facility where medical care was last authorized or provided. Individuals seeking information regarding access to claims and/or billing records will write to the VHA Chief Business Office Purchased Care, Privacy Office, PO BOX 469060, Denver, CO. All Requests for records about another person are required to provide a Request for an Authorization to Release Medical Records or Health Information signed by the record subject by using form VA Form 10–5345.

SORN ‘‘VHA Corporate Data Warehouses— VA’’ (172VA10) lists record access and contesting: Individuals seeking information regarding access to and contesting of records contained in this system of records may write to the Director of National Data Systems (105HIG), Austin Information Technology Center, 1615 Woodward Street, Austin, TX 78772. Inquiries should include the person’s full name, Social Security number, location and dates of employment or location and dates of treatment, and their return address.

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.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information.
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a "Statement of Disagreement"
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information.

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

Additional notice is provided through the SORNs listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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.

Redress is provided as indicated above in question 7.3.

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 individuals may seek to access or redress records about them held by the PIT system and may not know the procedure to accomplish the task.

Mitigation: Individuals are notified via the Notice of Privacy Practices, the SORNs and this PIA.

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?

Per VA Directive and Handbook 6500 every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls. OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring are performed using VA's Talent Management System (TMS).

VA form 9957 is used when creating accounts and granting appropriate access. Account access will be managed through the internal 9957 process which authorizes users of the information system and specifying access privileges. PIT uses Active Directory (AD) Service Desk Management (SDM) to determine access to sites within the application.

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?

There are no other agencies with 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.

SSRS Reporting Tool User Roles and Privileges

Role	Privileges
Administrator	Sets access to group reports/objects for Power User.
Report Author	Creates standard/ad-hoc reports for PIT, creates/modifies business rules in partnership with Chief of Program Integrity.
Information User	Views and utilizes existing reports in Business Intelligence Tool.

DataStage User Roles and Privileges

Role	Privileges
Administrator	Manages environments and version releases, maintains data integrity, and assists developer with designing ETL processes. Can create new data structures. Can execute system reports for capacity, performance, etc.
ETL Developer	Formulates data models, creates/maintains tables in data repository, specifies data mapping from source-to-target tables, develops ETL processing capabilities.
Operator	Can manually run ETL jobs, view ETL processing reports and statistics.

WODM User Roles and Privileges

Role	Privileges
Administrator	Full administrative rights on Decision Center, including the ability to define users and permissions. Plus, all Reviewer capabilities.
Reviewer	Able to review rules with status “Defined” and either approve them by assigning a status of “Validated”, reject them by assigning a status of “Rejected”, or launch them by assigning a status of “Deployable”. Plus, all Author capabilities.
Author	Able to author and modify business rules and assign a status of “Defined” to rules. Plus, all Viewer capabilities.
Viewer	Able to browse and view defined rules and schemes. (**NOTE:** the VA Claims Clerk will continue to use existing VA source systems to see claim line scores).

Role	Privileges
Administrator	The Administrator Role grants users' full administrative rights to the FAMS application, including the ability to run the Profile Baseline Processes including Service-Level Extract (SLE), Value Set generation and Profiling. The FAMS Administrators can: • Administer security. • Load and maintain claim database tables (with the partnership of the individual maintaining the PIT Enterprise Data Repository, as needed). • Define and create Auto-Extract Processes for Service Level Files. • Perform application data mapping to support the Auto-Extract process and feature selection Post-installation validation. • Participate in Defining Peer Group and Models. • Assist business users with selecting peer groups for review. • Define filters that FAMS administrators should apply to profiles. • Generate SLE extraction of claims from the Data Mart. • Generate Feature Values (answers to the questions in the scoring model). • Profile data, apply Hypothesis Modules, and provide values and scores for Business Users.
Business User	• Create behavior models. • Define and document custom report requirements. • Perform production testing. • Leverage the visualization, data discovery, and reporting capabilities within FAMS to identify outliers. • Create case notes and rosters within FAMS and assign cases for business use. • Review case information selected by FAMS Power Users. • Leverage FAMS reports to confirm allegations. • Print/store all reports required for case creation.

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.

Contractor access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system is required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access is required to complete additional role-based training prior to gaining system administrator access.

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.

All users with access to VA sensitive information or information system must complete VA Privacy and Security Awareness Rules of Behavior Training (TMS#10176) initially and annually thereafter. Personnel who access 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 reaffirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics Role-based Training Includes but is not limited to and based on the role of the user:
    - VA 1016925: Information Assurance for Software Developers IT Software Developers
    - VA 3193: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
    - VA 1357084: Information Security Role-Based Training for Data Managers
    - VA 64899: Information Security Role-Based Training for IT Project Managers
    - VA 3197: Information Security Role-Based Training for IT Specialists
    - VA 1357083: Information Security Role-Based Training for Network Administrators
    - VA 1357076: Information Security Role-Based Training for System Administrators
    - VA 3867207: Information Security Role-Based Training for System Owners.

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:* 8/26/2021

3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 9/30/2021
5. *The Authorization Termination Date:* 9/24/2024
6. *The Risk Review Completion Date:* 9/8/2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Not Applicable

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)*

Yes. VA Enterprise Cloud (VAEC) Azure

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.*

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.

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.

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).

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.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.06.13 13:46:52 -04'00'

Privacy Officer, Nancy Katz-Johnson

ERIC BAILEY

Digitally signed by ERIC BAILEY
Date: 2024.06.13 08:43:04 -04'00'

Information System Security Officer, Eric Bailey

TONY SINES

Digitally signed by TONY SINES
Date: 2024.06.13 07:28:25 -05'00'

Information System Owner, Tony Sines

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).

- Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES
- 23VA10NB3, Non-VA Care (Fee) Records-VA - (7-30-2015)
- 172VA10, VHA Corporate Data Warehouse-VA (12/22/2021)
- Privacy Act System of Records Notices (SORNs) site: https://department.va.gov/privacy/system-of-records-notices/

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