Privacy Impact Assessment for the VA IT System called:

Enterprise Legacy Database Community Care

Veterans Health Administration

Office of Integrated Veteran Care

Date PIA submitted for review:

8/1/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michael Hartmann	Michael.Hartmann@va.gov	303-780-4753
Information System Security Officer (ISSO)	Anthony McFarlane	Anthony.McFarlane2@va.gov	303-398-7155
Information System Owner	Sale Tunoascanlan	Sale.Tunoascanlan@va.gov	202-382-2338

Abstract

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

The Oracle database is the legacy repository for nearly all Community Care claim processing. Incoming claims, claim statuses, claim advice, are captured in the database. Several applications that adjudicate claims and process payments interface with the Oracle databases to read and write claim related data either by direct online connectivity or batch processing. Professional, Institutional, Dental, Medicare Crossover and Pharmacy claims are processed into the Claim Processing Eligibility (CP&E), Attachment Retrieval System (ARS) Assessing/ Electronic Web Viewer (EWV), Fee Payment Processing System (FPPS) Assessing, and Operational Decision Manager (ODM). These applications shared the database, but none wholly owned the database. Now these applications are moving to the cloud, but the Oracle database is not included in any of the application cloud provisioning allotments. Without the database, these production applications cannot run.

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. *The IT system name and the name of the program office that owns the IT system.*

Enterprise Legacy Database Community Care. Office of Integrated Veteran Care (IVC)

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

The system the business purpose of the database is captures and parceled for Processing claim data, for Providers and Veterans, health care claims and their payments. Enterprise Legacy Database Community Care (Claims Database) is expected to store over one billion records of individuals in the database.

C. *Indicate the ownership or control of the IT system or project.*

VA Owned and VA Operated

2. *Information Collection and Sharing*

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

The system is expected to store over one billion records of individuals in the database.

E. *A general description of the information in the IT system and the purpose for collecting this information.*

The system houses all 837 incoming claim transactions, all 835 outgoing claim transactions, and a multitude of data tables and elements associated with the incremental processing of those transactions between Community Care systems, and other entities including those authorized internal and external to the Department of Veterans Affairs.

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

The System will process all 835 outgoing claim transactions, and a multitude of data tables and elements associated with the incremental processing of those transactions between Community Care systems, and other entities including those authorized internal and external to the Department of Veterans Affairs.

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

The system will operate in the Enterprise Cloud (VAEC) Amazon Web Services (AWS).

3. Legal Authority and SORN

H. *A citation of the legal authority to operate the IT system.*

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)

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

Yes, SORN is over 6 years old and out of date, SORN POC is aware and working on update

D. System Changes

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

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

K. *Whether the completion of this PIA could potentially result in technology changes*

The completion of this PIA will not potentially 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.

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*
□ 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)

Data of Death, Member Identification Number, Patient Control Number, Medical Record Identification Number, Plan/Policy Number, Member Identification, Plan Name, Coverage Effective Dates, Coverage Limits, Co-pays, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Place of Service (Name), Place of Service Address (Street, City, Zip, Country), Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes.

PII Mapping of Components (Servers/Database)

Enterprise Legacy Database Community Care (Claims Database) consists of 1 key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Enterprise Legacy Database Community Care (Claims Database) 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
Claims Database	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Street Address, City, Zip Code, Country, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Plan/Policy Number,	Data is used to track, store, and process Veteran healthcare claims.	Data is encrypted at rest and in transit.

				Member Identification, Plan Name, Coverage Effective Dates, Coverage Limits, Co-Pays, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Tax Identification Number (TIN),Phone Number, Place of Service (POS) Name, Place of Service Address (Street, City, Zip, Country),Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription		

			Number, NCPDP Codes, (National Council For Prescription Drug Programs)		

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?

Ultimately, the data is sourced from a Veteran, but that information is provided to an industry provider who then submits the data to the VA via a clearing house transmission. The ClaimsDB application is a privacy sensitive system that collects, maintains, and makes available to the healthcare claim adjudication process healthcare related data for Veteran.

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.

ClaimsDB is a database is captures and parceled for Processing claim data, for Providers and Veterans, health care claims and their payments. Enterprise Legacy Database Community Care (Claims Database) is expected to store over one billion records of individuals in the database.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

Not Applicable, system does not create information.

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

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

The sources of information collected are ultimately the Beneficiary and providers and transmitted via Secure Sockets Layer (SSL).

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

Not applicable, the information is not collected by the system 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.

Data sources input information from the original source of the information is then verify and validated for accuracy when it was entered into the system. The system processes the information, it does not check the information for accuracy.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

System does not utilize a commercial aggregator of information to operate or function, and it does not check the information for accuracy.

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

(https://www.oprm.va.gov/privacy/systems_of_records.aspx).

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015) 24VA10A7, Patient Medical Records - VA (10/2/2020) 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015) 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021) 79VA10, Veterans Health Information Systems and

Technology Architecture (VistA) Records - VA (12/23/2020) 147VA10, Enrollment and Eligibility Records - VA (8/17/202

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: Unauthorized access or disclosure of Personally Identifiable Information (PII).

Mitigation: Depending on level of authority granted to the authorized administrators will have a specific level of access base on permission sets. The permissions will be reviewed on a regular basis to ensure that appropriate information is shared with appropriate users. Employs the standard VA required security measures designed to ensure that the information is not inappropriately disclosed or released.

Section 2. Uses of the Information

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

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

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

The information is used to support Incoming claims, claim statuses, claim advice, are captured in the database. Several applications that adjudicate claims and process payments interface with the Oracle databases to read and write claim related data either by direct online connectivity or batch processing:
•Name, •Social Security Number (SSN), •Date of Birth (DOB), •Data of Death (DOD), •Street Address, •City, •Zip Code, • Country, •Email, •Member Identification Number, • Patient Control Number, •Medical Record Identification Number, • Medical Record Number, •Plan/Policy Number, •Member Identification, •Plan Name, •Coverage Effective Dates, •Coverage Limits, •Co-Pays, •International Code Designator (ICD), •Coded Billing Information (Claim Index), •Billed Amounts, •Other Health Insurance Information, •Other Health Insurance FMS Document ID, •Tax Identification Number (TIN), •Phone Number, •Place of Service (POS) Name, •Place of Service Address (Street, City, Zip, Country), •Date of Service, •Charge Amount, •Paid Amount, •Diagnosis Codes, •Treatment Codes, •Prescription Number, •NCPDP Codes (National Council For Prescription Drug Programs.

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 system does not perform analysis on the data, it does not create or make available new or previously unutilized information about an individual.

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?

For Data at Rest, the storage device used to collect, process and/or retain information to include Social Security Numbers is an Encrypted Storage Array which is FIPS-140 compliant. For Data in Transit, the database uses Oracle Native Network Encryption to protect data in transit. It provides all data network encryption and integrity to ensure that data is secure as it travels across the network from Client to Database server and back.

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

All data is encrypted at rest and in transit to protect PII not limited SSNs. All connections must be approved prior to connection. The system is only accessed through VA Intranet by means of GFE laptops, Citrix Access Gateway (CAG), VA workstations. All three means of access are subject to standard VA encryption. Appropriate security controls are in place to guard against unauthorized access to the data.

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

System data is encrypted at rest and in transit at or above the VA requirements. The Technical Safeguards used to protect PII/PHI data are, two factor authentication (2FA), authorized access through the VA intranet only, the 15-minute timeout/session lock. For elevated privileges approval is required before an Electronic Permissions Access System (ePAS) can be submitted for approval.

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?

Access to PII is determined by the approved access level and role. The process is through the e9957 process. Local approval from supervisors and designated authorization officials are required prior to granting access to the database. No user can request access for themselves.

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

Yes, all employees and contractors with access to Veterans' information are required to complete VA Rules of Behavior and VA Privacy and Security training annually. Disciplinary actions, up to and including termination of employment, are possible for violations of the requirements specified in the training and their positions. These access rights are removed and reassigned for each transferred user, and these access permissions are re-approved annually

2.4c Does access require manager approval?

Access is processed through the e9957 process. Local approval from supervisors and designated authorization officials are required prior to granting access to the database.

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

Yes, through the use of tools and resources provided by the VA audits of modifications, creations, and deletes are monitored and recorded to an audit record.

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

All users of the system are responsible for assuring safeguards for the PII. The system manager is responsible for assigning users to the appropriate user roles to limit access and assuring PII safeguards as documented in the technical documentation and system design documentation.

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*

Data will be stored in the VAEC (VA Enterprise Cloud). The information is used to support Incoming claims, claim statuses, claim advice, are captured in the database. Several applications that adjudicate claims and process payments interface with the Oracle databases to read and write claim related data either by direct online connectivity or batch processing:
Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Street Address, City, Zip Code, Country, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Plan/Policy Number, Member Identification, Plan Name, Coverage Effective Dates, Coverage Limits, Co-Pays, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Tax Identification Number (TIN),Phone Number, Place of Service (POS)

Name, Place of Service Address (Street, City, Zip, Country),Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes,.

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.*

Yes. 1260.1, Care in Community, Temporary, destroy 6 years after all individuals in the record become ineligible for program benefits.

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.
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, (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf)

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

Yes, Item Number 1260.1, Care in the Community, Disposition Authority N1-15-03-1, Item 2

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.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items/ Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. https://www.va.gov/vapubs

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.

The system does not use PII information for research, testing, or training.

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: The risk of information contained in the Database may be retained for longer than necessary to fulfil the VA mission. Records retained longer then required may be at risk of unauthorized disclosure or breached.

Mitigation: To mitigate the risk posed by information retention, the Database adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in General Records Schedule.

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 Attachment Retrieval System (ARS)	Veteran healthcare claim data that includes all PII and all related PHI values which support claim adjudication	Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Street Address, City, Zip Code, Country,	Batch access TCP. System in internal to the VA. Only approved employees and contractors have

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***
EDI Web Viewer (EWV)		Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Plan/Policy Number, Member Identification, Plan Name, Coverage Effective Dates, Coverage Limits, Co-Pays, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Tax Identification Number (TIN), Phone Number, Place of Service (POS) Name, Place of Service Address (Street, City, Zip, Country), Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes (National Council For Prescription Drug Programs)	access to the system

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 Fee Payment Processing System (FPPS)	Veteran healthcare claim data that includes all PII and all related PHI values which support claim adjudication	Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Street Address, City, Zip Code, Country, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Plan/Policy Number, Member Identification, Plan Name, Coverage Effective Dates, Coverage Limits, Co-Pays, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Tax Identification Number (TIN), Phone Number, Place of Service (POS) Name, Place of Service Address (Street, City, Zip, Country), Date of Service,	Batch access TCP. System in internal to the VA. Only approved employees and contractors have access to the system

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***
		Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes (National Council For Prescription Drug Programs)	
Veterans Health Administration Healthcare Informatics Veterans Data Integration and Federation Enterprise Platform (VDIF-EP)	Veteran healthcare claim data that includes all PII and all related PHI values which support claim adjudication	Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Street Address, City, Zip Code, Country, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Plan/Policy Number, Member Identification, Plan Name, Coverage Effective Dates, Coverage Limits, Co-Pays, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information,	Batch access TCP. System in internal to the VA. Only approved employees and contractors have access to the system

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***
		Other Health Insurance FMS Document ID, Tax Identification Number (TIN), Phone Number, Place of Service (POS) Name, Place of Service Address (Street, City, Zip, Country), Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes (National Council For Prescription Drug Programs)	
Veterans Health Administration Claims Processing & Eligibility (CP&E)	Veteran beneficiary healthcare claim data that includes all PII and related PHI values. Data exchanged supports claim adjudication	Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Street Address, City, Zip Code, Country, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Plan/Policy Number, Member Identification, Plan Name, Coverage Effective Dates,	Batch access TCP. System in internal to the VA. Only approved employees and contractors have access to the system

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*
		Coverage Limits, Co-Pays, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Tax Identification Number (TIN), Phone Number, Place of Service (POS) Name, Place of Service Address (Street, City, Zip, Country), Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes(National Council For Prescription Drug Programs)	
Veterans Health Administration Payer EDI TAS (PED)	ClaimsDB is a database is captures and parceled for Processing claim data, for Providers and Veterans, health care claims and their payments. Enterprise Legacy Database Community Care (Claims Database) is expected to store over one billion	Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Street Address, City, Zip Code, Country, Email, Member Identification Number, Patient Control Number,	Batch access TCP. System in internal to the VA. Only approved employees and contractors have access to the system

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***
	records of individuals in the database.	Medical Record Identification Number, Medical Record Number, Plan/Policy Number, Member Identification, Plan Name, Coverage Effective Dates, Coverage Limits, Co-Pays, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Tax Identification Number (TIN), Phone Number, Place of Service (POS) Name, Place of Service Address (Street, City, Zip, Country), Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes (National Council For Prescription Drug Programs)	

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: There is a risk that information may be shared with unauthorized VA personnel.

Mitigation: Privacy risks to the information is minimized through various layers of security boundaries. The system resides in the security VAEC AWS with FIPS-140 encryption enabled. VAEC AWS practices continuous monitoring through audit and accountability measures, contingency planning, personnel security, awareness and training identification and authentication system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

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***
Globalscape (Change Healthcare Operations)	Veteran and beneficiary PII and PHI claim related data. Data exchanged supports initial receipt of healthcare claims from an industry clearing house through final disposition of processed payments to an industry clearing house. Claims include professional, institutional and dental	Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Street Address, City, Zip Code, Country, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Plan/Policy Number, Member Identification, Plan Name, Coverage Effective Dates, Coverage Limits, Co-Pays, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Tax Identification Number (TIN), Phone Number,	System MOU/ISA	Site to Site (S2S)

			Place of Service (POS) Name, Place of Service Address (Street, City, Zip, Country), Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes (National Council For Prescription Drug Programs)		

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: Sharing of information outside of the VA is only done when there is an approved connection, and MOU/ISA is in place. VAEC implements Federal Risk and Authorization Management Program (FedRAMP) approved security measures. Additionally, access to the system is monitored and restricted to personnel with both Multi-Factor Authentication and assigned permissions.

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.

Collection of information is done outside the accreditation boundary of the Claims Database, it only receives electronic data. While notice is not provided directly to individuals the system is using their data contained in other VA IT systems, this PIA does serve as notice of the system's existence and its SPI collection use, maintenance, and dissemination practices. The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided through the official System of Records Notice (SORN). VHA Systems of Records Notice: https://www.govinfo.gov/content/pkg/FR-2015-03 03/pdf/2015-04312.pdf

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

The system does not collect information from individuals. The sources collecting the information provide this notice. It is the responsibility of the providers to provided notice to each individual with a Patient Data Sharing Consent Form before collection of the information.

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

The system does not collect information from individuals. The sources collecting the information provide this notice. It is the responsibility of the providers to provided notice to each individual with a Patient Data Sharing Consent Form before collection of the information

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.

The system does not collect information from individuals. The sources collecting the information provide this notice. It is the responsibility of the providers to ensure the individuals understand their right to decline to provide the information. The notice to each individual with a Patient Data Sharing Consent Form before collection of the information

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.

The system does not collect information from individuals. The sources collecting the information provide this notice. It is the responsibility of the providers to ensure the individuals are provided the opportunity and right to decline to provide 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:

<u>Privacy Risk</u>: The individual may be unaware or not understand why their information is being collected.

<u>Mitigation</u>: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries when there is a change in regulation. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online.

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 system does not collect information from individuals. The sources collecting the information provide this notice. The rights of the Individuals to request access to review their records by use of the Records Notices (which are published in the Federal Register) 23VA10NB3 and 54VA10NB3 the location where a person may request records about themselves. First party would be a Privacy Act Request, 3rd party requests can only be processed with a signed authorization to disclose using a VHA-10-5345- Request for and Authorization to Release Medical Records or Health Information. All other requests would fall under the FOIA regulation as outlined in the U.S. Department of Justice Guide to the Freedom of Information Act.

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 does not collect information from individuals. The sources collecting the information provide this notice. Individuals have the rights to request access to review their records by submitting the VHA-10-5345 provides the process to Request for and Authorization to Release Medical Records or Health Information.

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

The system does not collect information from individuals. The sources collecting the information provide this notice. Individuals have the rights to request access to review their records by submitting the VHA-10-5345 provides the process to Request for and Authorization to Release Medical Records or Health Information.

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

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

The system does not collect information from individuals. The sources collecting the information provide this notice. Individuals are informed of the amendment process by many resources to include the Notice of Privacy Practice (NOPP). The procedure for correcting inaccurate or erroneous information begins with a Veteran requesting the records in question from Release of Information (ROI). The Veteran then crosses out the information they feel is inaccurate or erroneous from the records and writing in what the Veteran believes to be accurate. The request for amendment and correction is sent to the facility Privacy Office for processing. The documents are then forwarded to the practitioner who entered the data by the facility Privacy Officer. The practitioner either grants or denies the request. The Veteran is notified of the decision via letter by the facility Privacy Officer.

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.

The system does not collect information from individuals. The sources collecting the information provide this notice. Veterans are informed of the amendment process by resources to include the 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.

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.

The system does not collect information from individuals. The sources collecting the information provide this notice. Veterans and individuals should use the formal redress procedures addressed above.

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 the individuals may not know how to obtain access to their records or how to request corrections to their records.

Mitigation: As stated in section 7.3, the Notice of Privacy Practice (NOPP), which every patient signs prior to receiving treatment, discusses the process for requesting an amendment to one's records. Beneficiaries are reminded of this information when obtaining a copy of the NOPP. The VA Release of Information (ROI) office is available to assist Veterans with obtaining access to their medical records and other records containing personal information.

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.

There are no general users, only administrators for the Database. All administrators must complete the e9957 (Access Request Form) for access and must complete required training in the Talent Management System (TMS). The approved e9957 then is forward to the development team and an account creation request is created in Service Now (SNOW) to document the record creation. The approved e9957 is attached the SNOW ticket.

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?

Access is requested per VA policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes.

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.

There are no general users; only administrators for the Database. Administrator/Privileged Accounts are separate from the SUA and are Non-Mailbox Enabled Accounts (NMEA). Guest, Anonymous or Temporary accounts are not permitted.

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 who provide support to the system are required to complete annual training covering VA Privacy, Non-Disclosure Agreement (NDA) and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS). Background investigation and adjudication is completed on contract personnel serving in this role. Contractors will be given access to the system and complete their contractual obligations with role bases access control enforced. Contractors' credentials and certifications are reviewed quarterly by the Contract Officer Representative (COR).

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.

Initial and annual Security Awareness Training includes Privacy, HIPAA and VA Privacy and Information Security Awareness and Rules of Behavior. All required VA privacy training must be completed in TMS prior to the user being provisioned.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* The Security Plan Status: IOC 9/29/2023
2. *The System Security Plan Status Date:* The System Security Plan Status Date: IOC 9/29/2023
3. *The Authorization Status:* The Authorization Status: Authorization to Operate (ATO) IOC 9/29/2023
4. *The Authorization Date:* The Authorization Date: IOC 9/29/2023
5. *The Authorization Termination Date:* The Authorization Termination Date: IOC 9/29/2024
6. *The Risk Review Completion Date:* The Risk Review Completion Date: IOC 9/29/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* The FIPS 199 classification of the system (LOW/MODERATE/HIGH): IOC 8/18/2023

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)*

Claims Database utilizes cloud technology and is hosted within the VA Enterprise Cloud (VAEC), AWS GovCloud, which is a FedRAMP approved environment.

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.*

N/A. Claims Database utilizes cloud technology and is hosted within the VA Enterprise Cloud (VAEC), AWS GovCloud, which is a FedRAMP approved environment

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.

N/A. Claims Database utilizes cloud technology and is hosted within the VA Enterprise Cloud (VAEC), AWS GovCloud, which is a FedRAMP approved environment

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.

N/A. Claims Database utilizes cloud technology and is hosted within the VA Enterprise Cloud (VAEC), AWS GovCloud, which is a FedRAMP approved environment

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

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

N/A. Claims Database utilizes cloud technology and is hosted within the VA Enterprise Cloud (VAEC), AWS GovCloud, which is a FedRAMP approved environment

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.

MICHAEL HARTMANN

Digitally signed by MICHAEL HARTMANN
Date: 2023.10.24 11:06:24 -06'00'

Privacy Officer, Michael Hartmann

ANTHONY MCFARLANE

Digitally signed by ANTHONY MCFARLANE
Date: 2023.10.17 13:49:40 -06'00'

Information System Security Officer, Anthony McFarlane

SALE TUNOASCANLAN

Digitally signed by SALE TUNOASCANLAN
Date: 2023.10.17 13:26:54 -04'00'

Information System Owner, Sale Tunoascanlan

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).

- Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES
- 23VA10NB3, Non–VA Care (Fee) Records – VA (7/30/2015)
- 24VA10A7, Patient Medical Records – VA (10/2/2020)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
- 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, (11/8/2021)v
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
- 147VA10, Enrollment and Eligibility Records - VA (8/17/2021)

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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