Privacy Impact Assessment for the VA IT System called:

Attachment Retrieval System Assessing (ARS-Cloud)

Office of Information and Technology

Office of Integrated Veteran Care

eMASS ID #: 1203

Date PIA submitted for review:

08/26/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Eller Pamintuan	Eller.Pamintuan@va.gov	303-331-7512
Information System Security Officer (ISSO)	Paul Bartholomew	Paul.Bartholomew@va.gov	402-995-3858
Information System Owner	Dena Liston	Dena.Liston@va.gov	304-886-7367

Abstract

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

Attachment Retrieval System Assessing (ARS-Cloud) is a processing application and central repository for electronic supplemental healthcare claim data – that is 275 transactions from a healthcare clearinghouse. The parser component of ARS-Cloud matches attachments to specific claims, tags them for ease of retrieval, saves them to AWS S3 storage and records their access path in the Payer EDI Claims Oracle database. For each attachment, ARS-Cloud creates a 999 acknowledgement to return to the clearinghouse. It enables searching and viewing of attachments in its own web-based Graphical User Interface (GUI) and allows stored attachments to be retrieved from within Electronic Web Viewer (EWV). ARS-Cloud will notify the Electronic Data Interchange (EDI team) via an Outlook mail group when attachments are received that cannot be linked to a claim.

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?
Attachment Retrieval System Assessing (ARS-Cloud) will reside in the VAEC Amazon Web Services (AWS) cloud. Office of Integrated Veteran Care (IVC).

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

Ability to deliver Community Care Payer business services. The solution supports Veterans Administration (VA) funded industry provided services to Veterans, as well as supports VA funded industry provided services to Veteran beneficiaries. Key to timely payments to industry Providers providing Veteran service-related services.

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

VA Owned and VA Operated IS

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?

Attachment Retrieval System Assessing (ARS-Cloud) supports approximately 660,000+ Veterans and beneficiaries. Receives health care claims and translate and pass them to the destination systems

that conduct the transactions. System does not make payment transactions but contains claims data. Processing is automated; no individuals are involved.

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

ARS-Cloud is a central repository and retrieval vehicle for electronic attachments which provide supplemental claim information necessary to claim adjudication. It contains a parser that processes incoming 275 transaction batches sent from Change HealthCare Clearinghouse (CHC) to EDI Gateway. ARS validates attachments by matching them to claims, stores attachments in a central repository, records attachment IDs in the ARS database, saves information to the Program Tracking/Central Server database for distribution to Fee Basis Claims Systems (FBCS), and creates acknowledgement batches for return to CHC. It provides search and view capability for attachments in its web-based Graphical User Interface (GUI) and allows attachments to be identified and accessed from within EWV and FPPS. In addition, the IDs of attachments received for a claim are sent to VistA Fee Basis through FBCS (via Central Server) so that claims adjudicators have an indication that attachments exist for any claim they are working. In addition, ARS notifies the EDI team via an Outlook mail group when attachments are received that cannot be linked to a claim.

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

ARS-Cloud is a processing application and central repository for electronic supplemental healthcare claim data – that is 275 transactions from a healthcare clearinghouse. Information will be shared as identified in Section 4.1 and Section 5.1. Which when in transit, is secured via sFTP with Transport Layer Security Data. Data is encrypted at rest and in transit.

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?

Backups of the ARS Cloud system software and the data are intact and available at the alternate Amazon Web Services (AWS) and PII is maintained consistently in all sites and the same controls are used across sites.

3. Legal Authority and SORN

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

SORN numbers applicable to Payer EDI TAS are listed below:

24VA10A7, Patient Medical - VA (10-2-2020);
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1-25-2021); https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01526.pdf 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11-8-2021); https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020); https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf 88VA244, Centralized Accounts Receivable System/Centralize Accounts Receivable ON-Line System (CAR/CAROLS, combine system referred to as CAO) - VA (8-13-2018); https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf 147VA10, Enrollment and Eligibility Records - VA (8-17-2021); https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

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

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

4. System Changes

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

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

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

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. 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:

- Patient Name
- Social Security Number (SSN)
- Date of Birth (DOB
- Data of Death (DOD)
- Address
- Zip Code
- 2nd Address
- 2nd Zip Code
- Email, Member Identification Number
- Patient Control Number
- Medical Record Identification Number
- Medical Record Number
- Health Insurance Numbers (Policy Number)
- Coverage Dates
- Plan Name
- CPT and International Code Designator (ICD)
- Coded Billing Information (Claim Index)

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

- Billed Amounts
- Other Health Insurance Information
- Other Health Insurance FMS Document ID
- Paid Amounts
- Check or Remittance Numbers
- Provider Name
- Provider Phone Number
- Provider Billing Address
- Provider Physical Address
- Provider Remit to Address)
- Tax Identification Number, Diagnosis Codes
- Treatment Codes
- Prescription Numbers
- NCPDP Codes
- Date of Service (DOS)
- Place of Service (POS)
- Other Health
- Business phone
- Bank routing/account numbers
- VA ID
- Password
- Access Expiration

PII Mapping of Components (Servers/Database)

ARS-Cloud consists of **2** key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **ARS-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
Oracle Claims Database	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Date of	Data is used to track, store, and	Data is encrypted at rest and in transit.

			Death (DOD), Address, Zip Code, email, Member Identification Number, Sponsor Name, Sponsor Address, Patient Control Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Tax Identification Number (TIN), Place of Service (POS) Name, POS Address, Data of Server, Charge Amount, Diagnosis Codes, Treatment Codes, Prescriptions Number, NCPDP Codes	process Veteran healthcare claims.	
Claim Attachments	Yes	Yes	Name, Social Security Number	Data is used to	Data is encrypted at

			(SSN), Date of Birth (DOB), Date of Death (DOD), Address, Zip Code, email, Member Identification Number, Sponsor Name, Sponsor Address, Patient Control Number, Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address, Provider Tax Identification Number (TIN), Place of Service (POS) Name, POS Address, Data of Server, Charge Amount, Diagnosis Codes, Treatment Codes, Prescriptions Number, NCPDP Codes	track, store, and process Veteran healthcare claims.	rest and in transit.

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. As a component of Payer Electronic Data Interchange (EDI) Transactions Application Suite (TAS) of processing, the application is a central repository and retrieval vehicle.

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.

ARS-Cloud is a central repository and retrieval vehicle for electronic attachments which provide supplemental claim information necessary to claim adjudication. It contains a parser that processes incoming 275 transaction batches sent from Change HealthCare Clearinghouse (CHC) to EDI Gateway. ARS validates attachments by matching them to claims, stores attachments in a central repository, records attachment IDs in the ARS database, saves information to the Program Tracking/Central Server database for distribution to Fee Basis Claims Systems (FBCS), and creates acknowledgement batches for return to CHC. It provides search and view capability for attachments in its web-based Graphical User Interface (GUI) and allows attachments to be identified and accessed from within EWV and FPPS. In addition, the IDs of attachments received for a claim are sent to VistA Fee Basis through FBCS (via Central Server) so that claims adjudicators have an indication that attachments exist for any claim they are working. In addition, ARS notifies the EDI team via an Outlook mail group when attachments are received that cannot be linked to a claim.

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

ARS-Cloud is a central repository and retrieval vehicle for electronic attachments which provide supplemental claim information necessary to claim adjudication. ARS validates attachments by matching them to claims, stores attachments in a central repository, records attachment IDs in the ARS database, saves information to the Program Tracking/Central Server database for distribution to Fee Basis Claims Systems (FBCS), and creates acknowledgement batches for return to CHC.

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?

ARS-Cloud is a central repository and retrieval vehicle for electronic attachments which provide supplemental claim information necessary to claim adjudication. ARS validates attachments by matching them to claims, stores attachments in a central repository, records attachment IDs in the ARS database, saves information to the Program Tracking/Central Server database for distribution to Fee Basis Claims Systems (FBCS), and creates acknowledgement batches for return to CHC. The sources of information collected are ultimately the Beneficiary and industry providers and transmitted via secure SSL.

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?

ARS-Cloud does not collect information on a form. Information is provided to a industry providers who then submits the data to the VA via Secure Sockets Layer (SSL) transmissions.

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.

ARS-Cloud data is subject to a variety of internal edits and reconciliations. Reports aggregating claim activity are developed according to standard VHA controls. The system performs batch and real-time processing and moves data between tables and modifies data within the tables to make processed data reportable.
Upstream processing employs commercially acquired integrity checks that reject claims and supplemental claim data non-compliant with industry standard X12 transaction formats. Electronic rejections are transmitted to industry healthcare providers via an industry clearinghouse contracted by the Office of Community Care. Only valid transaction data is added to ARS-Cloud data stores for ARS-Cloud processing. Invalid transaction data never reaches ARS-Cloud processing.

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?

ARS-Cloud does not utilize a commercial aggregator of information to operate or function, and it does not check the information for accuracy. The system has a number of commercially acquired integrity checks that automatically reject claims that do not meet HIPAA mandated

requirements. If a claim is not properly developed the system rejects the claim and the clearinghouse must go back to the provider to correct the information prior to acceptance by VA.

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 numbers applicable to Payer EDI TAS are listed below:

24VA10A7, Patient Medical Records – VA (10/2/2020) 43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records – VA (1/25/2021) 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) – VA (12/23/2020) 88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018) 147VA10, Enrollment and Eligibility Records – VA (8/17/2021)

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u>

If the system collects more 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 than necessary to complete specific claim processing requirements, then any data breach would maximize Veteran data exposure.

Mitigation:

The information contained within the system is obtained indirectly from industry healthcare providers for the specific purpose of Veteran and beneficiary healthcare claim processing. Data collection is restricted to only those data elements required to adjudicate a claim and process a remittance. The system contains industry standard coded data and complies with the Health Insurance Portability and Accountability Act (HIPAA) requirements. The system is scanned by National Security Operations Center NSOC for vulnerabilities and those vulnerabilities are addressed to the extent possible. The system is only accessible by authorized staff on the VA network. The system is unreachable without approved remote access protocols from the outside world. All incoming and outgoing data to and from the system is sent through Federal Information Processing Standard (FIPS) 140-2 approved encryption.

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
Patient Name	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Social Security Number (SSN)	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Member Identification Number	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Patient Control Number	To ensure attachment records accuracy	To support electronic payment of health care claims.
Medical Record Identification Number	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.

Medical Record Number	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Address	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Zip Code	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Date of Birth (DOB)	To properly identify, adjudicate and pay	To support electronic payment of health care claims.
Date of Death (DOD)	To properly identify, adjudicate and pay	To support electronic payment of health care claims.
2nd Address	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
2nd Zip Code	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Plan Name	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Email	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Health Insurance Numbers (Policy Number)	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Coverage Dates	To provide actual dates for adjudication and pay claims	To support electronic payment of health care claims.
Date of Service (DOS)	To provide actual dates for adjudication and pay claims	To support electronic payment of health care claims.
Place of Service (POS)	To provide actual dates for adjudication and pay claims	To support electronic payment of health care claims.
CPT and International Code Designator (ICD	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Coded Billing Information (Claim Index)	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.

Billed Amounts	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Other Health Insurance Information	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Other Health Insurance FMS Document ID	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Prescription Numbers	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
NCPDP Codes	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Provider Name	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Provider Phone Number	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Provider Billing Address	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Provider Physical Address	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Provider Remit to Address	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Treatment Codes	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Paid Amounts	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Check or Remittance Numbers	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Tax Identification Number (TIN), Diagnosis Codes	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Other Health	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.

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?

ARS-Cloud does not have the capability to analyze data, it does not produce the data. It contains a parser that processes incoming 275 transaction batches sent from Change HealthCare Clearinghouse (CHC) to EDI Gateway. ARS validates attachments by matching them to claims, stores attachments in a central repository, records attachment IDs in the ARS database, saves information to the Program Tracking/Central Server database for distribution to Fee Basis Claims Systems (FBCS), and creates acknowledgement batches for return to CHC.

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 information but rather serves as a processing system and central repository for electronic attachments as identified above in section 1.2.

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 Network Encryption protects data in transit. It provides all data network encryption and integrity to ensure that data is secure as it travels across the network.

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

Data in transit is protected by means of industry standard encryption protocols (e.g., HTTPS, VPN, etc.). Data at rest is FIPS 140-3 compliant and fully encrypted at aggregate-level. All data is encrypted while at rest and during transmission. 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?

The information contained within the system is obtained indirectly from industry healthcare providers for the specific purpose of Veteran and beneficiary healthcare claim processing. Data collection is restricted to only those data elements required to adjudicate a claim and process a remittance. The system contains industry standard coded data and complies with the Health Insurance Portability and Accountability Act (HIPAA) requirements. The system is scanned by National Security Operations Center NSOC for vulnerabilities and those vulnerabilities are addressed to the extent possible. The system is only accessible by authorized staff on the VA network. The system is unreachable without approved remote access protocols from the outside world. All incoming and outgoing data to and from the system is sent through Federal Information Processing Standard (FIPS) 140-2 approved encryption.

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

Access to PII is limited by the ARS application to only those data items deemed necessary for a user to perform their job, as determined by their management team and their job description.
System documentation includes detailed system design and user guides that specify those areas of the system that contain PII and PHI, as well as how it is to be used by the user. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function.

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 system.

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

Yes, it is the responsibility of the project making the request to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities or operates. (Including but not limited to: VA 6500, TIC, PIA/PTAs, SORN, and application ATO.

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

- Patient Name: to properly identify, adjudicated and pay claims
- Social Security Number (SSN): to properly identify, adjudicated and pay claims
- Member Identification Number: to properly identify, adjudicated and pay claims
- Patient Control Number: to ensure attachment records accuracy
- Medical Record Identification Number: to properly identify, adjudicated and pay claims
- Medical Record Number: to properly identify, adjudicated and pay claims

- Date of Birth (DOB): to properly identify, adjudicated and pay claims
- Date of Death (DOD): to properly identify, adjudicated and pay claims
- Address: to properly identify, adjudicated and pay claims
- Zip Code: to properly identify, adjudicated and pay claims
- 2nd Address: to properly identify, adjudicated and pay claims
- 2nd Zip Code: to properly identify, adjudicated and pay claims
- Email: to properly identify, adjudicated and pay claims
- Health Insurance Numbers (Policy Number): to properly identify, adjudicated and pay claims
- Coverage Dates: to provide actual dates for adjudication and pay claims
- Plan Name: to properly identify, adjudicated and pay claims
- Date of Service (DOS): to provide actual dates for adjudication and pay claims
- Place of Service (POS): to provide actual place for adjudication and pay claims
- CPY and International Code Designator (ICD) Coded Billing Information: to properly identify, adjudicated and pay claims
- Other Health Insurance Information: to properly identify, adjudicated and pay claims
- Other Health Insurance FMS Document ID: to properly identify, adjudicated and pay claims
- Prescription Numbers: to properly identify, adjudicated and pay claims
- NCPDP Codes Information: to properly identify, adjudicated and pay claims
- Coded Billing Information (Claim Index): to properly identify, adjudicated and pay claims
- Billed Amounts: to properly identify, adjudicated and pay claims
- Treatment Codes: to properly identify, adjudicated and pay claims
- Diagnosis Codes: to properly identify, adjudicated and pay claims
- Paid Amounts: to properly identify, adjudicated and pay claims
- Check or Remittance Numbers: to properly identify, adjudicated and pay claims
- Tax Identification Number: to properly identify, adjudicated and pay claims
- Provider Name: to properly identify, adjudicated and pay claims
- Provider Phone Number: to properly identify, adjudicated and pay claims
- Provider Billing Address: to properly identify, adjudicated and pay claims
- Provider Physical Address: to properly identify, adjudicated and pay claims
- Provider Remit to Address: to properly identify, adjudicated and pay claims
- Other Health: to properly identify, adjudicated and pay claims

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. Retention schedule has been approved by the VHA Record Control Schedule and the National Archives and Records Administration (NARA). Retention period is 6 years, and destroyed 7 years after final payment or cancellation, but longer retention is authorized if required for business use.

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, records are maintained and disposed of in accordance with records disposition authority.
VHA RCS 10-1: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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

Yes, the retention schedule has been approved by the VHA Record Control Schedule and the National Archives and Records Administration (NARA) GRS 1.1: Financial Management and Reporting Records General Records Schedule 6 Item 10a.

VHA RCS 10-1: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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 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 Handbook 6500.1, Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the Deleted Items or 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 and NIST SP800-88r1 as evidenced in the FedRAMP Audit reports. Additionally, the system adheres to the retention of records as required by VA Handbook 6300.1 (Records Management Procedures) and VA Directive 6300 (Records and Information Management).

Users with Directorate's designated records liaison are required to maintain and dispose of records, according to the VHA approved records schedules. Retirement of records requires the use of a VA Form 7468, Request for Disposition of Records, which is authorized for paper and local electronic records.

The application will follow NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process of any IT storage hardware used in the ARS application. The Guidelines establish three levels of data destruction: Clear, Purge, and Destroy, that can be applied to different data storage devices. An appropriate destruction method will be chosen based on the memory type (Flash Memory, Magnetic Drives, Optical Devices, Hard Copies etc.) used for the storage. It is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws.

Regarding temporary paper records, those that contain PII, and VA sensitive information, which are under the jurisdiction of VA, will be handled securely, economically, and effectively and disposed of properly. Written documentation that attests to the completion of the destruction process after the final destruction is required, which could be in the form of a letter, memo, or any format attesting to its complete destruction. This certification is not considered a valid certification of destruction if completed and submitted before the final destruction of the records. The certification should contain sufficient information to attest to the final destruction of the temporary paper records – what temporary records were destroyed, the date when they were destroyed, what destruction method was used, where they were destroyed, and who was responsible for their final destruction.

Paper records are destroyed on site, destruction verification of secure shred containers is verified by the logistics department. The VHA Office of Integrated Veteran Care (IVC) program office has a current shredding contract. No documents leave the facility, and system users are unable to print from a remote location.

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.

Copies of production data are used for Pre-Production testing. Access to the Pre-Production environment and data is restricted to business personnel and less than five Independent Validation & Verification (IV&V) personnel. Established policies and procedures address this matter and each member has training to ensure they understand the risks while testing with the PII data. Training documentation is kept within the Training office. No connections shall be permitted without having an Enterprise Security External Change Council (ESECC) approval.

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:

If data is maintained within the ARS-Cloud system for a longer time than what is needed or required, then information may be compromised, breached, or unintentionally released to unauthorized individuals increases.

Mitigation:

The ARS-Cloud system adheres to information security requirements instituted by the VA OI&T to secure data with PII in a FISMA-Moderate environment. A Backup Plan and Restore Plan are in place. At a minimum, the plan includes the requirement to save data for the backup and recovery of information stored on the AWS infrastructure, and the retention of records as required by VA Handbook 6300.1 (Records Management Procedures) and VA Directive 6300 (Records and Information Management). Business Associate Agreements – Appropriate VA authorities/supervisors/managers assign Functional Categories to all contracts that may have exposure or access to VA Personal Health Information (PHI)/Personally Identifiable Information (PII) information. Functional Categories are verified annually. Talent Management System (TMS) training is required annually.

- VA 10176: VA Privacy and Information Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training

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***
Office of Information and Technology	IAM SSOi Service	VA ID, Password, Name, Access Expiration, Email, Phone Number	Via ssl https:// within the VA network.
Office of Information and Technology	eCAMS	Patient – Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD) Address (Street, City, Zip, Country), Patient Control Number, Medical Record Identification Number, Medical Record Number, etc. Provider – Name, Tax Identification Number (TIN), Physical Address (Street, City, Zip, Country), Billing Address (Street, City, Zip, Country), Remit to Address (Street, City, Zip, Country), Phone Number,	Batch processing of flat files containing healthcare claim related data; SFTP within the VA network.

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*
		Remit Amount, Bank Account Number	
Office of Veteran Integrated Care	MoveIT	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Phone Numbers, Email Addresses, Health Insurance Beneficiary Numbers, Account Numbers, Current Medications, Previous Medical Records	SFTP within the VA network

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:

If an end-user with an open ARS-Cloud session does not properly lock his/her GFE when stepping away, then unauthorized individuals may see or copy data from the ARS-Cloud GUI.

Mitigation:

The OI&T develops, disseminates, and periodically reviews and updates access control policies and procedures. OI&T has formally developed an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among other VA entities. The policies and procedures are reviewed on an annual basis by responsible parties and updated as needed. In addition, end-users must complete two required courses annually.

- Privacy and HIPAA Training.
- B.VA Privacy and Information Security Awareness and Rules of Behavior.

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***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

Privacy Risk:

N/A, no ARS-Cloud data is transferred to external entities.

Mitigation:

N/A, no ARS-Cloud data is transferred to external entities.

Section 6. Notice

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

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

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

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

The VA policy is not to disclose any personal information to third parties outside VA without their consent, or as authorized by law. Any questions or concerns regarding VA privacy policy or use of patient information can be made by contacting VA Privacy Service, or by mailing questions or concerns at Department of Veterans Affairs, Privacy Service, 810 Vermont Avenue, N.W. (005R1A) Washington, DC 20420.

VHA Notice of Privacy Practices is located here: VHA Notice of Privacy Practices

It is Veterans Health Administration (VHA) policy that the VHA Notice of Privacy Practices (Information Bulletin 10-163) is created, maintained, and distributed in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule at 45 C.F.R. § 164.520, to inform Veterans, beneficiaries, caregivers, and non-Veteran patients of the use and disclosure of their health information without authorization, their rights to access and restrictions on certain uses and disclosures and VHA's legal duties to maintain the privacy of their health information. AUTHORITY: 45 C.F.R. parts 160 and 164.

The SORN for CommCare CRM is as follows:

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

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

Payer EDI TAS does not collect information from the Veteran/Beneficiary. The sources collecting the information provide this notice. VHA Notice of Privacy Practices is located here: VHA Notice of Privacy Practices

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

This Privacy Impact Assessment (PIA) also serves as notice of the ARS-Cloud system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." Disclosure of Social Security numbers of those for whom benefits are claimed is requested under the authority of 38 USC and is voluntary. Social Security numbers will be used in the administration of Veterans' benefits and in the identification of Veterans or persons claiming or receiving VA benefits and their records and may be used for other purposes where authorized by 38 USC and the Privacy Act of 1974 (5 USC 552a) or where required by other statutes.

1. Beneficiaries are provided notice of privacy practices upon enrollment. A form of this notice is provided in the ChampVA Guide.
2. Privacy notices are provided at the point of service at the medical center where the Veteran and beneficiary receive care, in accordance with VHA Handbook 1605.4, Notice of Privacy Practices.
3. Notice of privacy practices are available on the VA Privacy website. https://www.oprm.va.gov/privacy/systems_of_records.aspxEach of the above notices includes information on how to report any use of information that is not in accordance with the collection. See Appendix A for the notice of privacy practices provided at all VA medical centers.

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.

Individuals do have the right to refuse to provide information but doing so may result in denial of the claim and/or inappropriate care to be provided. Yes, see Appendix A.

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

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

VHA Handbook 1605.1, Privacy and Release Information, paragraph 5 lists the Individual's rights of Veterans and Beneficiaries to request VHA to restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the records.

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:

If Veterans or their beneficiaries are not provided adequate notification that their PII and PHI healthcare related information is stored, maintained, and made available from a cloud-based application, then delayed awareness could create Veteran frustration leading to bad press.

Mitigation:

Privacy practice notices are provided to Veterans and their beneficiaries at the time of service. This is in accordance with (IAW) VHA Handbook 1605.04 NOTICE OF PRIVACY PRACTICES. Per the VHA Handbook 1605.04 Notice of Privacy Practices. All Programs that are administered by the Office of Integrated Veteran Care (IVC)) are provided these notices at least every 3 years. The Privacy Office retains a copy of the notices and how often they are provided to the Veteran.

Section 7. Access, Redress, and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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

VHA Directive 1605.01, Privacy and Release of Information states the rights of Veterans and Beneficiaries to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review or seek copies of records must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access to data must be delivered to, and reviewed by, the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must include the signature of the requester, date of birth, copy of signed government identification, state what is request and the period of the information requested. Mail requests for eligibility information/records to: CHAMPVA Eligibility PO Box 469028 Denver, CO 80246-9028. Mail requests for CHAMPVA billing/claim records to: VHA Office of Integrated Veteran Care Privacy/FOIA Office, PO Box 469060 Denver, CO 80246-9060. Requests for medical and pharmacy records contact your servicing medical provider and for Community Care authorizations/authorization numbers are located at the referring VA Medical Center. For Veteran claim payment information will need to be submitted to the VA Financial Services Center (FSC) Privacy Office by first contacting them via email at vafscprivacyofficer@va.gov for secure submission methods. For Veteran Explanation of Benefits maintained by the VA's Third-Party Administrators may be requested by the Veteran registering and requesting their records from either (TriWest Healthcare Alliance) (https://veteran.triwest.com/bizflowappdev/apps/veteranportal/?tz=GMT-0700) or Optum (https://veteran.vacommunitycare.com/start). Medical and pharmacy records should be sought from the medical facility where the patient received care.and Veteran and Beneficiary

(CHAMPVA) lien or subrogation requests should be submitted to the respective action office via the instructions located at https://www.va.gov/OGC/Collections.as

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

The system is not exempt.

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

VHA Directive 1605.01, Privacy and Release Information, paragraph 5 states the rights of Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access to ARS records must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

7.2 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.

Veterans and beneficiaries have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request must be mailed or delivered to the organization that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

Individuals have the right to request an amendment (or correction) to information in the ARS records if they believe it is incomplete, inaccurate, untimely, or unrelated to operations.

VHA Handbook 1605.1, Privacy and Release Information, paragraph 5 lists the rights of Veterans and Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operation.

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.

VHA Handbook 1605.1, *Privacy and Release of Information*, paragraph 5 states the rights of Veterans and Beneficiaries to amend their records by submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, which may be used as the written request requirement. This includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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

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

If a Veteran or Beneficiary discovers that incorrect information was provided during the intake process, they must submit an information amendment request. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.5.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:

Privacy Risk:

There is a risk that incorrect information is accidentally recorded in an individual's record. An individual may want to review the content of their record to check for data accuracy. The magnitude of harm associated with this risk to the VA is low.

Mitigation:

Application mitigates the risk by requiring all applicable Contractors and VA employees who engage with ARS to complete all of the following data security and privacy VA trainings: VA Privacy and Information Security Awareness and Rules of Behavior Training, and Privacy and HIPAA focused training. Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply.

Section 8. Technical Access and Security

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

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

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

8.1a Describe the process by which an individual receives access to the system?

The supervisor/Contracting Officer's Representative (COR) documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training. This documentation and monitoring is performed through the use of the Talent Management System (TMS). Access to the system is granted to VA employees and contractors the supporting IT for the application after the supervisor/COR authorizes this access once requirements have been met. Only the IT system administrators authorized by VA IT will have the security role to modify the ARS application. This PIA will not result in technology protocol changes, additional controls, or single sign on, as per privacy control AR-7, Privacy-Enhanced System Design and Development. All ARS users must take the following steps before they are granted access to the system:

- Individuals must take and pass training on VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203), and government ethics.

- Individuals must have a completed security investigation.
- After the training and the security investigation are complete, a request is submitted for access

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

There are no ARS users from other agencies; only VA employees and contractor are granted access.

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.

Developer Access: Developers account management processes should further ensure that only end users are able to access the environment. Developers and ARS Project teams will work to create, update, access and disable developer accounts for project teams. Additionally, there shall be a review of user access periodically to evaluate whether users are active in the environment; if the user is not active, their account is terminated. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. A designated VA Project Point of Contact (POC) is the only person who may submit account creation requests and submitted for accountability purposes.

End-User and Tester Access: All individuals requesting developer access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203)) and applicable role-based training. This may include but is not limited to Information Security for IT Specialists Training) and must be authorized by VA Project Manager. To ensure that this requirement is met, the designated VA Project POC must submit a signed Access Request Form for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the CommCare-CRM application Environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, current on VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Version date: October 1, 2023 Access Permissions, and Contract End date, access justification and completed training certifications.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

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

- Contractors must take and pass training on VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA10203), and government ethics and role-based training based on support role to the system.
- Contractors must have signed the Non-Disclosure Agreement (NDA) and Rules of Behavior (RoB).
- Contractors must have successfully completed VA contractor background security investigation as per the Position Designation Automated Tool (PDT).
- Once complete, a request is submitted for access. Before access is granted to the production environment; this request must be approved by the supervisor, and OIT.

VA owns the data that the ARS application extracts from the source applications, and Microsoft manages and secures the ARS application data. The VA and Microsoft Project Managers, CORs have weekly meetings for the review of the contract details and this contract is reviewed at least on an annual basis. There shall be a regular review of user access to evaluate whether users are active in the environment. If a user is not active, the account will be terminated. A designated VA Project POC is the only person who may submit account creation requests for accountability purposes. Contractor access to the system expires at the end of the contract duration or earlier.

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.

VA privacy and security training is mandatory.

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- VA 10176: VA Privacy and Information Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics

Role-based Training is based on the role of the user and includes, but is not limited to:

- 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: Pass
2. The System Security Plan Status Date: 12/26/2023
3. The Authorization Status: Authorization to Operate (ATO)
4. The Authorization Date: 2/25/2024
5. The Authorization Termination Date: 2/24/2025
6. The Risk Review Completion Date: 2/09/2024The FIPS 199 classification of the system (LOW/MODERATE/HIGH): MODERATE, MODERATE, MODERATE

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

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

No

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)*

VA Enterprise Cloud (VAEC) Amazon

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.

N/A

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

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).

The use RPAs or "bots" are not implemented within the ARS application.

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.

ELLER PAMINTUAN

Digitally signed by ELLER PAMINTUAN
Date: 2024.11.19 12:08:06 -07'00'

Privacy Officer, Eller Pamintuan

PAUL BARTHOLOMEW

Digitally signed by PAUL BARTHOLOMEW
Date: 2024.11.13 10:56:41 -06'00'

Information System Security Officer, Paul Bartholomew

DENA LISTON

Digitally signed by DENA LISTON
Date: 2024.11.13 11:45:21 -05'00'

Information System Owner, Dena Liston

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

The SORN for CommCare CRM is as follows:

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

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

VHA Notice of Privacy Practices is located here: VHA Notice of Privacy Practices

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