



Privacy Impact Assessment for the VA IT System called:

Attachment Retrieval System (ARS)-Cloud

Office of Information and Technology

Date PIA submitted for review:

June 7, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Christian Loftus	Christian.Loftus@va.gov	859-281-2470
Information System Security Officer (ISSO)	Richard Alomar-Loubriel	Richard.Alomar-Loubriel@va.gov	787-641-7582 x11411
Information System Owner	Christopher Brown	Christopher Brown1@va.gov	202-270-1432

Abstract

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

Attachment Retrieval System (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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, Vista, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*

- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? 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.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

ARS-Cloud will reside in the VAEC Amazon Web Services (AWS) cloud. Implementation of ARS-Cloud will support mechanics of claim adjudication and claim payments, but it will not change the overall policies and rules that govern VHA OCC business processes.

SORN numbers applicable to ARS-Cloud are listed below and are found at this link:

https://www.oprm.va.gov/docs/Current_SORN_List_10_13_2020.pdf

147VA10NF1, Enrollment and Eligibility Records-VA. Also, Privacy Notices provided in Program Guides and on the Program websites – July 14, 2016;

23VA10NB3, Non-VA Care (Fee) Records-VA – July 30, 2015;

24VA10P2, Patient Medical Records-VA – July 30, 2015;

38VA21, Veterans and Beneficiaries Identification Records Location Subsystem-VA (6-4-2001)

43VA008, Veterans, Service Members, Family Members, and VA Beneficiary Survey Records-VA (4-6-2007)

54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA 3/3/2015

79VA10P2, Veterans Health Information Systems and Technology Architecture (VistA) – VA (10-31-2012)

88VA244, Accounts Receivable Records – VA; 147VA16, Enrollment and Eligibility

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.

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:

- | | | |
|--|--|--|
| <input checked="" type="checkbox"/> Name | Number, etc. of a different individual) | <input checked="" type="checkbox"/> Previous Medical Records |
| <input checked="" type="checkbox"/> Social Security Number | <input checked="" type="checkbox"/> Financial Account Information | <input type="checkbox"/> Race/Ethnicity |
| <input checked="" type="checkbox"/> Date of Birth | <input checked="" type="checkbox"/> Health Insurance Beneficiary Numbers | <input checked="" type="checkbox"/> Tax Identification Number |
| <input type="checkbox"/> Mother's Maiden Name | Account numbers | <input checked="" type="checkbox"/> Medical Record Number |
| <input type="checkbox"/> Personal Mailing Address | <input type="checkbox"/> Certificate/License numbers | <input checked="" type="checkbox"/> Other Unique Identifying Number (list below) |
| <input type="checkbox"/> Personal Phone Number(s) | <input type="checkbox"/> Vehicle License Plate Number | |
| <input type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Internet Protocol (IP) Address Numbers | |
| <input type="checkbox"/> Personal Email Address | <input checked="" type="checkbox"/> Current Medications | |
| <input checked="" type="checkbox"/> Emergency Contact Information (Name, Phone | | |

Veterans or beneficiaries - Health Insurance Numbers, CPY 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, and National Provider Identifier (NPI), Dates of Service, Types of Service

PII Mapping of Components

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.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) 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
<p>AWS S3 Buckets</p> <p>via Production VM vac10appar1210 (va.gov domain)</p>	<p>Yes</p>	<p>Yes</p>	<p>Supplemental Medical Records (X-Rays, Test Results, 2nd Opinions, etc.) and other claim handling details for accurate claim processing are provided in PDF, JPG, TIF, GIF in HTM format. Records may contain:</p> <p><u>Patient</u> - Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD) Address (Street, City, Zip, Country), 2nd Address (Street, City, Zip, Country), Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, etc.</p> <p><u>Provider</u> - Name, Tax Identification Number (TIN),</p>	<p>Supplemental healthcare claim data facilitates accurate processing of Veteran healthcare claims.</p>	<p>Access is controlled via ARS.</p> <p>FIPS 2.0 Encryption.</p> <p>Data is encrypted at rest and in transit.</p>

			<p>Physical Address (Street, City, Zip, Country), Billing Address (Street, City, Zip, Country), Remit to Address (Street, City, Zip, Country), Phone Number, etc.</p> <p><u>Treatment/Service</u> – Place of Service (POS) Name, POS Address (Street, City, Zip, Country), Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes, etc.</p>		
<p>Oracle Claims Database oithacdbsfPRD02 (vha.med.va.gov domain)</p>	Yes	Yes	<p>Veteran healthcare claim data that includes all PII and all related PHI values which support claim adjudication.</p> <p><u>Patient</u> – Name, Social Security Number (SSN), Date of Birth (DOB), Date of Death (DOD) Address (Street, City, Zip, Country), 2nd Address (Street, City, Zip, Country), Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical</p>	Data is used to track, store, and process Veteran healthcare claims.	Data is encrypted at rest and in transit.

			<p>Record Number, etc.</p> <p><u>Health Insurance</u> – Plan/Policy Number, Member ID, Plan Name, Coverage Effective Dates, Coverage Limits and Co-Pays, and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Sponsor Name, Sponsor Address, etc.</p> <p><u>Treatment/Service</u> – Place of Service (POS) Name, POS Address (Street, City, Zip, Country), Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes, etc.</p>	
--	--	--	---	--

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Ultimately, the data is sourced from a Veteran or Veteran beneficiary, 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 ARS-Cloud application is a privacy sensitive system that collects, maintains, and makes available to the healthcare claim adjudication process healthcare related data for Veterans and beneficiaries. During claims processing additional information related to the claim is tagged with a Patient Document Identifier (PDI) for traceability to all related claims.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

As a component of Payer Electronic Data Interchange (EDI) Transactions Application Suite (TAS) of processing, the ARS-Cloud application is a privacy sensitive system that collects, maintains, and makes available to the healthcare claim adjudication process healthcare related data for Veterans and beneficiaries. Most of claim information is collected directly from healthcare service providers via the Change Healthcare Clearinghouse. A small percentage of claims are collected directly from Veterans or their beneficiaries via US Mail.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.

This question is related to privacy control AP-2, Purpose Specification.

Veteran and beneficiary personal and healthcare related information is collected and stored to ensure that healthcare services provided by industry providers is appropriate, eligible for reimbursement, and reimbursed in a timely fashion.

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

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.

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.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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.

1.6 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

This system supports electronic payment of health care claims and ensures VA is not in violation of the Health Insurance Portability and Accountability Act (HIPAA). The rules for data sharing are clearly laid out in the transactions sets and must be followed to the letter or claims will fail to process.

The ARS-Cloud system's legal authority for operating the system, specifically the authority to collect the information listed is Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725,

1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101. Notice is provided by the system’s System of Record Notice (SORN), Electronic Document Management System (EDMS)-VA, VA SORN 54VA10NB3: that covers Veterans, Dependents, Healthcare providers treating individuals and caregivers of Veterans which can be viewed at the following links: <https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf>
https://www.oprm.va.gov/docs/Current_SORN_List_05_28_2021.pdf

1.7 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.

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: If the system collects more 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 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.

ARS-Cloud delivers Community Care Payer business services. It's a fully automated system that enables retrieval of supporting documentation to facilitate and expedite adjudication of Veteran and beneficiary healthcare claims. ARS-Cloud currently contains data on approximately 780,000 Veterans and beneficiaries. Data includes PII, PHI and limited financial data (charges, billed amounts).

- 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
- Date of Birth (DOB)/Date of Death (DOD): to properly identify, adjudicated and pay claims
- Address; Zip Code: to properly identify, adjudicated and pay claims
- Health Insurance Numbers: to properly identify, adjudicated and pay claims
- Coverage Dates: to provide actual dates for adjudication 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
- Health Information (and other insurance): to properly identify, adjudicated and pay claims
- Prescription/NCPDP Codes Information: to properly identify, adjudicated and pay claims
- Procedure/Treatment/Diagnosis Codes Number/Coded Billing Information (Claim Index): to properly identify, adjudicated and pay claims
- Paid Amounts Information (Check/Remittance Numbers): to properly identify, adjudicated and pay claims
- Tax Identification Number: to properly identify, adjudicated and pay claims
- Provider Name, Phone, Billing Address, Physical Address: to properly identify, adjudicated and pay claims
- Provider's TIN: to properly identify, adjudicated and pay claims

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

On a daily basis, the "parser" component of ARS-Cloud receives incoming X12 275 transactions (aka supplemental claim data) for claims that have been, or will soon be, submitted to the VA for financial reimbursement. The parser searches E_REPOS tables in the claims database to identify a matching claim. Attachments for which a claim exists are properly tagged and stored in secure S3 storage (encrypted at rest). The location and key to that storage is then entered into ARS-Cloud tables in the claims database for easy retrieval by claims processors during adjudication and voucher examiners during audits.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

Add answer here:

There are two types of access control for two different needs.

1. Direct Access: Application End-User Access: PIV and ARS-Cloud User Role
 - A. 2FA Authentication. Users must have an active PIV card to login in.

- B. Application-Level Capability. Users must have some level business defined capability recorded in the ARS-Cloud tables of the claims database to get beyond the SSOi login and access functionality. To obtain this database defined level of capability, a supervisor or higher authority who is already authorized to use the application must submit a New User request within ARS-Cloud. That request is routed to the appropriate ARS-Cloud business administrator who can execute Create User functionality that identifies the new user and associated capabilities within ARS-Cloud tables in the claims database. Records here are searched and confirmed before allowing PIV-active users into the ARS application.
2. Indirect Access: Server administration: 2FA Authentication and eToken.
- Access requests are submitted and processed internally via MyVA/ePAS.
 - Any request must identify exact Roles and Active Directory (AD) groups required.
 - Any request must be approved by a “Tier” or “Role” above the requesting individual before undergoing additional approvals by appropriate AD owners/approvers.
 - Once processed, a password-enabled eToken is issued that must be inserted into the device used to access the server (in addition to the PIV card).

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
- Date of Birth (DOB)/Date of Death (DOD): to properly identify, adjudicated and pay claims
- Address; Zip Code: to properly identify, adjudicated and pay claims
- Health Insurance Numbers: to properly identify, adjudicated and pay claims
- Coverage Dates: to provide actual dates for adjudication 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
- Health Information (and other insurance): to properly identify, adjudicated and pay claims
- Prescription/NCPDP Codes Information: to properly identify, adjudicated and pay claims
- Procedure/Treatment/Diagnosis Codes Number/Coded Billing Information (Claim Index): to properly identify, adjudicated and pay claims
- Paid Amounts Information (Check/Remittance Numbers): to properly identify, adjudicated and pay claims

- Tax Identification Number: to properly identify, adjudicated and pay claims
- Provider Name, Phone, Billing Address, Physical Address: to properly identify, adjudicated and pay claims
- Provider's TIN: 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.

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) GRS 1.1: Financial Management and Reporting Records General Records 1.1, Item 10: **Temporary**. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.

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

GRS: <https://www.archives.gov/records-mgmt/grs.html>

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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.

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

GRS: <https://www.archives.gov/records-mgmt/grs.html>

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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, (April 8, 2014), <https://www.va.gov/vapubs>

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** (November 3, 2008), <https://www.va.gov/vapubs>. 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. Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research? This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Only advance-authorized business end-users are permitted over-the-shoulder training with current business end-users. 9957-approved Independent Verification & Validation (IV&V) personnel are allowed access to ARS-Cloud production data. 9957-approved Production Support personnel do not directly access ARS-Cloud production data but may be exposed to it during investigation of a production processing incident.

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.

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. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
IAM SSOi Service	OIT Identity and Access Management	End-user credentials: VA ID, Password, Name, Access Expiration, Email, Phone Number	Via ssl https:// within the VA network. (TCP/IP)
eCAMS	Healthcare claim data that includes PII and related PHI is to identify supplemental data related to specific claims to facilitate remittance processing.	<p><u>Patient</u> – Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD) Address (Street, City, Zip, Country), 2nd Address (Street, City, Zip, Country), Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, etc</p> <p><u>Provider</u> – 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, Remit Amount, Bank Account Number, etc.</p>	Batch processing of flat files containing healthcare claim related data.
Movelt Utility	Pass through vehicle. Transfers transactions from clearinghouse to ARS. 275 transactions include all types of PII and PHI.	<p><u>Patient</u> – Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD) Address (Street, City, Zip, Country), 2nd Address (Street, City, Zip, Country), Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, etc.</p>	SFTP

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
		<p><u>Health Insurance</u> – Plan/Policy Number, Member ID, Plan Name, Coverage Effective Dates, Coverage Limits and Co-Pays, and International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Sponsor Name, Sponsor Address, etc.</p> <p><u>Treatment/Service</u> – Place of Service (POS) Name, POS Address (Street, City, Zip, Country), Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes, etc.</p>	

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.

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.

- A. 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: This question is #7 in the Privacy Threshold Analysis.

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

No ARS-Cloud supplemental claim data is transferred to external entities.

Data Shared with External Organizations

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external</i>	<i>List the method of transmission and the measures in place to secure data</i>
--	---	--	---	---

	<i>program office or IT system</i>		<i>sharing (can be more than one)</i>	
N/A	N/A	N/A	N/A	N/A

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

All data is encrypted while at rest and during transmission. Appropriate security controls are in place to guard against unauthorized access to the data.

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: N/A

Mitigation: N/A

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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 question is 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.

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.aspx

Each 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

Veterans and beneficiaries have the right to request restrictions on use and disclosure of all or part of their healthcare information. Disclosures and use of information or disclosure restrictions are under the provisions of the 45 CFR and the VA Notices of Privacy Practices that provide the necessary details for requesting or releasing information of their records. Veterans must submit a written request that identifies information they want restricted and the extend of the restriction being requested. 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. See **Appendix A** for additional details regarding the consent and practices.

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.

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 Community Care (OCC) 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?

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.

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).

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. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

See **Appendix A** for the notice of privacy practices provided at all VA medical centers, which includes the following:

Right to Review and Obtain a Copy of Health Information. You have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care.

NOTE: Please send a written request, to your VHA health care facility Privacy Officer. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314)801-0800. The Web site is [Veteran's Service Records](#).

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.

See **Appendix A** for the notice of privacy practices provided at all VA medical centers, which includes the following:

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

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

- File an appeal
- File a "Statement of Disagreement"

- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

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.

See **Appendix A** for the notice of privacy practices provided at all VA medical centers, which includes the following:

Right to Request Receipt of Communications in a Confidential Manner. You have the right to request that we provide your health information to you by alternative means or at an alternative location. We will accommodate reasonable requests, as determined by VA/VHA policy, from you to receive communications containing your health information:

- At a mailing address (e.g., confidential communications address) other than your permanent address
- In person, under certain circumstances

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.

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

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

Individuals have a right to contact the VHA call center to gain access to their information. 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.

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.

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: If rigorous application access controls are not implemented for ARS-Cloud, then Veteran personal data becomes susceptible to hackers in our expanding electronic world.

Mitigation: Users are first authenticated via approved VA 2FA credentials, and then further restricted by role-based-assignment access to only the data needed to process a claim. Hacking attempts are thwarted through a multifaceted approach of NSOC manned firewalls and gateways, AD account requirements, role-based assignments and login credentials.

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?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Access to the ARS-Cloud system is limited to authorized users. VA staff who have completed the required training and agreed to Rule of Behavior will gain access on a need-to-know basis. All user accounts allow read only access to data. All users must be VA cleared.

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 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.

Yes, VA is highly dependent on contract augmentation of its workforce. However, contractors must go through background checks, sign the Rules of Behavior and have the same restrictions as VA staff.

The Office of Information and Technology (OIT) is responsible for ensuring that all contractors who are working on OIT projects have signed Non-Disclosure Agreements and met any necessary contractual requirements governing access and handling of Veteran data.

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?

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

The ARS-Cloud Authority to Operation (ATO) has been granted a 1-year ATO, with an ATO termination date of April 1, 2022. The FIPS 199 Classification of the system is MODERATE.

Section 9. 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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

Privacy Officer, Christian Loftus

Information Systems Security Officer, Richard Alomar-Loubrie

System Owner, Christopher Brown

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).

Veterans' Health Administration NOTICE OF PRIVACY PRACTICES Effective Date September 23, 2013 https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090

https://www.opm.va.gov/privacy/systems_of_record.aspx

Department of Veterans Affairs-Veterans Health Administration

NOTICE OF PRIVACY PRACTICES

Effective Date September 23, 2013

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED OR DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY.

The Department of Veterans Affairs' (VA) Veterans Health Administration (VHA) is required by law to maintain the privacy of your protected health information and to provide you with notice of its legal duties and privacy practices. VHA is also required to abide by the terms of this Notice and its privacy policies.

How VHA May Use or Disclose Your Health Information without Your Authorization

(See below for more information about these categories)

- Treatment (e.g., giving information to VHA and other doctors and nurses caring for you)
- Payment (e.g., giving information to non-VHA facilities that provide care or services)
- Health Care Operations (e.g., giving information to individuals conducting Quality of Care reviews)
- Eligibility and Enrollment for VA Benefits (e.g., giving information to officials who decide benefits)
- Abuse Reporting (e.g., giving information about suspected abuse of elders or children to government agencies)
- Health or Safety Activities
- Public Health Activities (e.g., giving information about certain diseases to government agencies)
- Judicial or Administrative Proceedings (e.g., responding to court orders)

- Law Enforcement
- Health Care Oversight (e.g., giving information to the Office of Inspector General or a Congressional Committee)
- Cadaveric Organ, Eye, or Tissue Donation
- Coroner or Funeral Activities
- Services (e.g., giving information to contractors or business associates performing services for VHA)
- National Security Matters
- Workers' Compensation Cases (e.g., giving information to officials who decide payments for workplace injuries Payment (e.g., giving information to non-VHA facilities that provide care or services)
- Correctional Facilities
- When Required by Law
- Activities Related to Research (e.g., certain activities with only minimal or limited privacy or confidentiality risks)
- Planning VA research projects (e.g., investigator accesses, but does not disclose or record, individual health information to determine feasibility of opening a study)
- Military Activities (e.g., giving information to the Department of Defense (DoD))
- Academic Affiliates (e.g., giving information to assist in training medical students)
- State Prescription Drug
- Monitoring Program (SPDMP) reporting and query
- General Information Disclosures (e.g., giving out general information about you to your family and friends)
- Verbal disclosures to others while you are present
- Verbal Disclosures when you are not present (e.g., assisting Family Members or Designated Individuals Involved in your Care)

Other Uses and Disclosures with Your Authorization. We may use or disclose your health information for any purpose based on a signed, written authorization you provide us. Your signed written authorization is always required to disclose your psychotherapy notes if they exist. If we were to use or disclose your health information for marketing purposes, we would require your signed written authorization. In all other cases, we will not use or make a disclosure of your health information without your signed, written authorization, unless the use or disclosure falls under one of the exceptions described in this Notice. When we receive your signed written authorization, we will review the authorization to determine if it is valid, and then disclose your health information as requested by you in the authorization.

Version Date: February 27, 2020

Page 31 of 35

Revocation of Authorization. If you provide us a written authorization or permission to use or disclose your health information, you may revoke that permission, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information except to the extent that VHA has relied on your written authorization. Please understand that we are unable to take back any uses or disclosures we have already made based on your authorization.

YOUR PRIVACY RIGHTS Right to Request Restriction.

You may request that we not use or disclose all or part of your health information to carry out treatment, payment or health care operations, or that we not use or disclose all or part of your health information with individuals such as your relatives or friends involved in your care, including use or disclosure for a particular purpose or to a particular person.

Please be aware, we are not required to agree to such restriction, except in the case of a disclosure restricted under 45 CFR § 164.522(a)(1)(vi). This provision applies only if the disclosure of your health information is to a health plan for the purpose of payment or health care operations and your health information pertains solely to a health care service or visit which you paid in full. However, VHA is not legally able to accept an out of pocket payment from a Veteran for the full cost of a health care service or visit. We are only able to accept payment from a Veteran for co-payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of your health information to a health plan for the purpose of receiving payment for health care services provided to you.

To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. If we agree to your request, we will honor the restriction until you no longer make the restriction request valid or you revoke it.

NOTE: We are not able to honor requests to remove all or part of your health information from the electronic database of health information that is shared between VHA and DoD, or to restrict access to your health information by DoD providers with whom you have a treatment relationship.

Right to Review and Obtain a Copy of Health Information. You have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care.

NOTE: Please send a written request, to your VHA health care facility Privacy Officer. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314)801-0800. The Web site is <http://www.archives.gov/veterans/military-service-records/medical-records.html>.

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

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

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

Right to Receive an Accounting of Disclosures. You have the right to know and request a copy of what disclosures of your health information have been made to you and to other individuals outside of VHA. To exercise this right, you must submit a written request to the facility Privacy Officer at the VHA health care facility that provides your care.

Right to a Printed Copy of the Privacy Notice. You have the right to obtain an additional paper copy of this Notice from your VHA health care facility. You can obtain this Notice from the facility Privacy Officer at your local VHA health care facility. You may also obtain a copy of this Notice at the following website, http://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1089

Notification of a Breach of your Health Information. If a breach of any of your protected health information occurs, we will notify you and provide instruction for further actions you should take, if any.

Complaints. If you are concerned that your privacy rights have been violated, you may file a complaint with:

- The VHA health care facility's Privacy Officer, where you are receiving care. Visit this Web site for VHA facilities and telephone numbers http://www1.va.gov/directory/guide/division_flash.asp?dnum=1.
- VA via the Internet through "Contact the VA" at <http://www.va.gov>; by dialing 1-800-983-0936 or by writing the VHA Privacy Office (10P2C1) at 810 Vermont Avenue NW, Washington, DC 20420.
- The U.S. Department of Health and Human Services, Office for Civil Rights at <http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html>
- The Office of the Inspector General. <http://www.va.gov/oig/contact/default.asp>
- Complaints do not have to be in writing, though it is recommended.
- An individual filing a complaint will not face retaliation by any VA/VHA organization or VA/VHA employee.

Changes. We reserve the right to change this Notice. The revised privacy practices will pertain to all existing health information, as well as health information we receive in the future. Should there be any changes we will make available to you a copy of the revised Notice within 60 days of any change.

When We May Use or Disclose Your Health Information without Your Authorization Treatment.

We may use and disclose your health information for treatment or to provide health care services. Treatment may include:

- Emergency and routine health care or services, including but not limited to labs and x-rays; clinic visits; inpatient admissions
- Contacting you to provide appointment reminders or information about treatment alternatives
 - Prescriptions for medications, supplies, and equipment
 - Coordination of care, including care from Non-VHA providers
 - Coordination of care with DoD, including electronic information exchange

NOTE: If you are an active duty service member, Reservist or National Guard member, your health information is available to DoD providers with whom you have a treatment relationship. Your protected health information is on an electronic database that is shared between VHA and DoD. VHA does not have the ability to restrict DoD's access to your information in this database, even if you ask us to do so.

Examples:

- 1) A Veteran sees a VHA doctor who prescribes medication based on the Veteran's health information. The VHA pharmacy uses this information to fill the prescription.
- 2) A Veteran is taken to a community hospital emergency room. Upon request from the emergency room, VHA discloses health information to the non-VHA hospital that needs the information to treat this Veteran.
- 3) A National Guard member seeks mental health care from VHA. VHA discloses this information to DoD by entering the information into a database that may be accessed by DoD providers at some future date.

Payment. We may use and disclose your health information for payment purposes or to receive reimbursement for care provided, including: Determining eligibility for health care services

- Paying for non-VHA care and services, including but not limited to, CHAMPVA and fee basis
- Coordinating benefits with other insurance payers
- Finding or verifying coverage under a health insurance plan or policy
- Pre-certifying benefits
- Billing and collecting for health care services provided
- Providing personal information to consumer reporting agencies regarding delinquent debt owed to VHA
- Allowing you to pay for your health care out of pocket so that your insurance is not billed

Examples:

- 1) A Veteran is seeking care at a VHA health care facility. VA uses the Veteran's health information to determine eligibility for health care services.
- 2) The VHA health care facility discloses a Veteran's health information to a private health insurance company to seek and receive payment for the care and services provided to the Veteran.

Health Care Operations. We may use or disclose your health information without your authorization to support the activities related to health care, including:

- Improving quality of care or services
- Conducting Veteran and beneficiary satisfaction surveys
- Reviewing competence or qualifications of health care professionals
- Providing information about treatment alternatives or other health-related benefits and services
- Conducting health care training programs
- Managing, budgeting and planning activities and reports
- Improving health care processes, reducing health care costs and assessing care costs and assessing organizational performance
- Developing, maintaining and supporting computer systems
- Legal services
- Conducting accreditation activities
- Certifying, licensing, or credentialing of health care professionals
- Conducting audits and compliance programs, including fraud, waste and abuse investigations

Examples:

- 1) Medical Service, within a VHA health care facility, uses the health information of diabetic Veterans as part of a quality of care review process to determine if the care was provided in accordance with the established best clinical practices.
- 2) A VHA health care facility discloses a Veteran's health information to the Department of Justice (DOJ) attorneys assigned to VA for defense of VHA in litigation.

Eligibility and Enrollment for Federal Benefits. We may use or disclose your health information to other programs within VA or other Federal agencies, such as the Veterans Benefits Administration, Internal Revenue Service or Social Security Administration, to determine your eligibility for Federal benefits.

Abuse Reporting. We may use or disclose your health information without your authorization to report suspected child abuse, including child pornography; elder abuse or neglect; or domestic violence to appropriate Federal, State, local, or tribal authorities. This reporting is for the health and safety of the suspected victim.

Health and Safety Activities. We may use or disclose your health information without your authorization when necessary to prevent or lessen a serious threat to the health and safety of the public, yourself, or another person. Any disclosure would only be to someone able to help prevent or lessen the harm, such as a law enforcement agency or the person threatened. You will be notified in writing if any such disclosure has been made by a VHA health care facility.

Public Health Activities. We may disclose your health information without your authorization to public health and regulatory authorities, including the Food and Drug Administration (FDA) and Centers for Disease Control (CDC), for public health activities. Public health activities may include:

- Controlling and preventing disease, injury, or disability
- Reporting vital events such as births and deaths
- Reporting communicable diseases such as hepatitis, tuberculosis, sexually transmitted diseases & HIV
- Tracking FDA- Regulated products
- Enabling product recalls, repairs or replacements
- Reporting adverse events and product defects or problems

Judicial or Administrative Proceedings. We may disclose your health information without your authorization for judicial or administrative proceedings, including:

- We receive an order of a court, such as a subpoena signed by a judge, or administrative tribunal, requiring the disclosure
- To defend VA in judicial and administrative proceedings

Law Enforcement. We may disclose your health information to law enforcement agencies for law enforcement purposes when applicable legal requirements are met. These law enforcement purposes may include:

- Identifying or apprehending an individual who has admitted to participating in a violent crime
- Routine reporting to law enforcement agencies, such as gunshot wounds

Health Care Oversight. We may disclose your health information to a governmental health care oversight agency (e.g., Inspector General; House Veterans Affairs Committee) for activities authorized by law, such as audits, investigations, and inspections. Health care oversight agencies include government agencies that oversee the health care system, government benefit programs, other government regulatory programs, and agencies that enforce civil rights laws.

Cadaveric Organ, Eye, or Tissue Donation. When you are an organ donor and death is imminent, we may use or disclose your relevant health information to an Organ Procurement Organization (OPO), or other entity designated by the OPO, for the purpose of determining suitability of your organs or tissues for organ donation. If you have not specified your donation preferences and can no longer do so, your family may make the determination regarding organ donation on your behalf.

Coroner or Funeral Services. Upon your death, we may disclose your health information to a funeral director for burial purposes, as authorized by law. We may also disclose your health information to a coroner or medical examiner for identification purposes, determining cause of death, or performing other duties authorized by law.

Services. We may provide your health information to individuals, companies and others who need to see your information to perform a function or service for or on behalf of VHA. An appropriately executed contract and business associate agreement must be in place securing your information.

National Security Matters. We may use and disclose your health information without your authorization to authorized Federal officials for the purpose of conducting national security and intelligence activities. These activities may include protective services for the President and others.

Workers' Compensation. We may use or disclose your health information without your authorization to comply with workers' compensation laws and other similar programs.

Correctional Facilities. We may disclose your health information without your authorization to a correctional facility if you are an inmate and disclosure is necessary to provide you with health care; to protect the health and safety of you or others; or for the safety of the facility.

Required by Law. We may use or disclose your health information for other purposes to the extent required or mandated by Federal law (e.g., to comply with the Americans with Disabilities Act; to comply with the Freedom of Information Act (FOIA); to comply with a Health Insurance Portability and Accountability Act (HIPAA) privacy or security rule complaint investigation or review by the Department of Health and Human Services).

Activities Related to Research. Before we may use health information for research, all research projects must go through a special VHA approval process. This process requires an Institutional Review Board (IRB) to evaluate the project and its use of health information based on, among other things, the level of risk to you and to your privacy. For many research projects, including any in which you are physically examined or provided care as part of the research, you will be asked to sign a consent form to participate in the project and a separate authorization form for use and possibly disclosure of your information. However, there are times when we may use your health information without an authorization, such as, when:

- A researcher is preparing a plan for a research project. For example, a researcher needs to examine patient medical records to identify patients with specific medical needs. The researcher must agree to use this information only to prepare a plan for a research study; the researcher may not use it to contact you or actually conduct the study. The researcher also must agree not to remove that information from the VHA health care facility. These activities are considered preparatory to research.

- The IRB approves a waiver of informed consent and a waiver of authorization to use or disclose health information for the research because privacy and confidentiality risks are minimal and other regulatory criteria are satisfied.
- A Limited Data Set containing only *indirectly* identifiable health information (such as dates, unique characteristics, unique numbers or zip codes) is used or disclosed, with a data use agreement (DUA) in place.

Military Activities. We may use or disclose your health information without your authorization if you are a member of the Armed Forces, for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, when applicable legal requirements are met. Members of the Armed Forces include Active Duty Service members and in some cases Reservist and National Guard members. An example of a military activity includes the disclosure of your health information to determine fitness for duty or deployment to your Base Commander.

Academic Affiliates. We may use or disclose your health information, without your authorization, to support our education and training program for students and residents to enhance the quality of care provided to you.

State Prescription Drug Monitoring Program (SPDMP). We may use or disclose your health information, without your authorization, to a SPDMP in an effort to promote the sharing of prescription information to ensure appropriate medical care.

General Information Disclosures. We may disclose general information about you to your family and friends. These disclosures will be made only as necessary and, on a need, -to-know basis consistent with good medical and ethical practices, unless otherwise directed by you or your personal representative. General information is limited to:

- Verification of identity
- Your condition described in general terms (e.g., critical, stable, good, prognosis poor)
- Your location in a VHA health care facility (e.g., building, floor, or room number)

Verbal Disclosures to Others While You Are Present. When you are present, or otherwise available, we may disclose your health information to your next-of-kin, family or to other individuals that you identify. For example, your doctor may talk to your spouse about your condition while at your bedside. Before we make such a disclosure, we will ask you if you object. We will not make the disclosure if you object.

Verbal Disclosures to Others When You Are Not Present. When you are not present, or are unavailable, VHA health care providers may discuss your health care or payment for your health care with your next-of-kin, family, or others with a significant relationship to you without your authorization. This will only be done if it is determined that it is in your best interests. We will limit the disclosure to information that is directly relevant to the other person's involvement with your health care or payment for your health care. Examples of this type of disclosure may include questions or discussions concerning your in-patient medical care, home-based care, medical supplies such as a wheelchair, and filled prescriptions.

***IMPORTANT NOTE:** A copy of your medical records can be provided to family, next-of-kin, or other individuals involved in your care only if we have your signed, written authorization or if the individual is your authorized surrogate (the individual who is authorized to make health care decisions on your behalf if you can no longer do so) and the practitioner determines that the information is needed for the individual to make an informed decision regarding your treatment.*

When We Offer You the Opportunity to Decline the Use or Disclosure of Your Health Information

Patient Directories. Unless you opt-out of the VHA medical center patient directory when being admitted to a VHA health care facility, we may list your general condition, religious affiliation and the location where you are receiving care. This information may be disclosed to people who ask for you by name. Your religious affiliation will only be disclosed to members of the clergy who ask for you by name. If you do object to being listed in the Patient Directory, no information will be given out about you unless there is other legal authority. This means your family and friends will not be able to find what room you are in while you are in the hospital. It also means you will not be able to receive flowers or mail, including Federal benefits checks, while you are an inpatient in the hospital or nursing home. All flowers and mail will be returned to the sender.

When We Will Not Use or Disclose Your Health Information

Sale of Health Information. We will not sell your health information. Receipt of a fee expressly permitted by law, such as Privacy Act copying fees or FOIA fees is not a sale of health information.

Genetic Information Nondiscrimination Act (GINA). We will not use genetic information to discriminate against you either through employment or to determine your eligibility for VA benefits.

Contact Information.

You may contact your VHA health care facility's Privacy Officer if you have questions regarding the privacy of your health information or if you would like further explanation of this Notice. The VHA Privacy Office may be reached by mail at VHA Privacy Office, Office of Informatics and Analytics (10P2C1), 810 Vermont Avenue NW, Washington, DC 20420 or by telephone at 1-877-461-5038.