Privacy Impact Assessment for the VA IT System called:

PAPER MAIL CONVERSION AND MANAGEMENT SERVICES (PMCMS)

VETERANS BENEFITS ADMINISTRATION (VBA)

Date PIA submitted for review:

2 June 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jean-Claude Wicks	Jean-claude.wicks@va.gov	240-302-4321
Information System Security Officer (ISSO)	Richard Alomar-Loubriel	Richard.alomar-loubriel@va.gov	787-641-7582
Information System Owner	Derek Herbert	Derek.herbert@va.gov	202-461-9606

Abstract

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

The Veterans Benefits Administration (VBA) Paper Mail Conversion and Management Service (PMCMS) processes Personally Identifying Information (PII) and Personal Health Information (PHI/ePHI). Mail shipments of Veterans' physical documents are received at the scan vendor facility/facilities where they are prepared for scanning. Prepared documents are scanned and processed by VBA PMCMS as e-documents. This reduces paperwork and processing time for Veterans' claims and increases the ease and speed of access to their records. Hardcopy documents are held after scanning only as required to allow for review and any necessary re-scanning (to ensure high quality images) and are promptly and securely returned to the Department of Veterans Affairs custody.

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.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *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? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Paper Mail Conversion and Management Service (PMCMS) Centralized Mail Portal system is a proprietary system owned by Leidos and provided as a System as a Service (SaaS) to the Veterans Benefits Administration (VBA).

Converted centralized mail images and metadata represent a significant strategic asset for VA regarding completing Veteran claims for compensation and other benefits. As such, the Government currently

utilizes the PMCMS CM Portal to provide VA access to converted mail packets for manual and automated processing by VA and contracted resources.

The Paper Mail Conversion and Management Service (PMCMS) Centralized Mail Portal system is a proprietary system owned by Leidos and provided as a System as a Service (SaaS) to the Veterans Benefits Administration (VBA).

As of June 2022, the PMCMS CM Portal system contains data for 6.2 million Veterans. This data is collected to support Veteran and dependent claims for compensation and other benefits.

PMCMS CM Portal collects, scans, and disseminates to VBMS and maintains the following data for benefits claims adjudication and processing: Veteran File ID Number – information is collected for benefits claimant identification and routing); Veteran First Name - – information is collected for benefits claimant identification and routing); Veteran Middle Initial - – information is collected for benefits claimant identification and routing); Veteran Last Name - – information is collected for benefits claimant identification and routing); Veteran Mailing Address Zip Code - – information is collected for benefits claimant identification and routing). The following data is not stored as distinct data elements, but the information may appear on scanned document images that are transmitted from the CM Portal to VBMS: Veteran SSN; Veteran date of birth (DoB); Mailing address; Zip code; Phone number; Fax number; Email address; Emergency contact information; Health insurance beneficiary info; Current medication; Medical history; Race/ethnicity.

PMCMS collects first name, last name, Veteran file number and zip/international postal code from end users of the Direct Upload application. As documents are digitized and submitted to the system, additional SPI data is contained in PMCMS including spouse's Social Security Number (SSN); service-related disabilities; service information; retired/severance pay/pension information; marital and dependency information; income information; and medical and legal expenses. Data collected is necessary to establish, develop, decide, and pay a Veteran's claim. It directly supports the VA's VBA VBMS, a paperless claims system that greatly reduces the time required to process a case. The data is used only in support of the business purpose and according to contract stipulations, it is not used for any other purpose

VA VBA requires the use of or access to PMCMS CM Portal, and the Leidos PMCMS CM Portal system requires the use of VBMS, via an interconnection as approved by the VA Office of Information Technology (OIT) System Owner. The expected benefits of the interconnection are as follows: For Leidos PMCMS CM Portal to receive digitized VBA source documents and send them to VBMS. The interconnection will further support the input of information into the Content Management System eDocument Service so that it can be utilized by applications or other services.

The Leidos PMCMS CM Portal system is a cloud-based system hosted in AWS GovCloud. The system is deployed across multiple Virtual Private Clouds (VPCs) to separate front-end and back-end services and to segregate production from test systems. The PMCMS CM Portal is a primarily containerized, serverless microservices architecture with only a few virtual machines hosting services for database, scanning vendor interfaces, and management / systems administration functions. Leidos retains responsibility for the safeguarding of the data in our custody, while ownership of the data remains with the VA.

VA Contract VA118-16-D-1004 provides Leidos the authority to operate PMCMS CM Portal.

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

The completion of this PIA will not result in technology changes.

The system is not in the process of being modified. Therefore, the SORN #58VA21/22/28 will not require amendment or revision and approval. At this time the PMCMS program does not know if the VBMS infrastructure is cloud based.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Account Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Current Medications
- ☒ Previous Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integration Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin

☒ Other Unique Identifying Information (list below)

Additional SPI processed includes the VA File number; spouse's Social Security Number (SSN); service-related disabilities; service information; retired/severance pay/pension information; marital and dependency information; income information; and medical and legal expenses.

PII Mapping of Components

PMCMS consists of one database. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by PMCMS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
DMHS (CM Portal)	Yes	Yes	Name, SSN, DoB, mailing address, zip code, phone number, fax number, email address, emergency contact information, health insurance beneficiary info, current medication, medical history, race/ethnicity.	Transmission to VBMS	VA maintained S2S connection over an encrypted tunnel.

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.

In support of VBMS's primary mission of making Veteran's information gathering and processing more efficient, SMS/Leidos receives source materials directly from the following entities:

- Veterans,
- Veteran's Family Members,
- Veteran's representative,
- Third parties providing evidence in support of a claim,
- VBA Regional Offices (ROs), and
- Veterans Service Organizations (VSOs).

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.

Information processed by VBA PMCMS is gathered from a wide variety of originators and sources.

Documents may include both printed and handwritten content from:

- Paper (e.g., VA Form 21-526)
- Photographs

- Faxes.

Electronic format source materials may include, but are not limited to:

- eForms
- eFax
- CD/DVD
- Flash drives
- Microfilm
- Microfiche
- Other alternate media (e.g., 3.5" floppy disks)

The VA provides this information to support the conversion of documents from paper to e-

formats to optimize VBMS, a paperless claims processing system that greatly reduces the time required to establish, develop, decide, and pay claims. The data collected, used, disseminated, created, or maintained by VBA PMCMS as part of the DMHS (CM Portal) supports this purpose.

The VBA also implemented the PMR Retrieval Program to improve timeliness for the receipt of medical records in support of a Veteran's claim for disability benefits. Under the PMR process, conversion vendors receive medical release statements (VA Form 21-4142, 21-4142a, and other medical release of information authorizations) via physical mail, direct upload, secure file transfer, and fax. The vendors scan the medical release statements, convert the images to PDF format, and transfer the PDF files and metadata to the PMR vendor via an existing secure, automated, system-to- system process. The records are requested by the PMR vendor on behalf of the VA. In parallel, the conversion vendors upload the medical release statements to the VBMS eFolder, per the existing DMHS (CM Portal) process.

As the work is being completed by the PMR vendor, it is securely transferred back to the conversion vendor. The returned electronic documents include medical records/evidence received, letters, reports of contact, returned mail (in some instances), and reject notices. These are transferred back to the conversion vendors via the secure, automated system-to-system process. The artifacts and the processes directly support the VBA mission of making the claims process far more efficient.

1.4 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.

The information processed by VBA PMCMS (i.e., converted to e-copy) is systematically checked for accuracy against the original hardcopy provided by the source. Any requirement to assess the accuracy of the data provided to the source by a Veteran is beyond the operational requirements of the system. The accuracy of transmitted and stored data is ensured via the use of checksum/encryption standards (which meet FIPS 140-2 approval).

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

The legal authority includes Title 20 Chapter IX Part 1001, and the authorization for operation of VBA PMCMS is VA Contract No. VA118-11-D-1000, and Title 38, United States Code, section 501(a) and Chapters 11, 13, 15, 18, 23,30, 31, 32, 34, 35, 36, 39, 51, 53, 55 VBAPMCMS SON995C/SOI VA08, Exhibit 300 # 029-00-01-22-01-1265-00, VBA Systems of Records Notice (SORN) # 58VA21/22/28.

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

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

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

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

<u>Principle of Data Quality and Integrity:</u> Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

The processing of Name, SSN, DoB, mailing address, zip code, phone number, fax number, email address, emergency contact information, health insurance beneficiary info, current medication, medical history, race/ethnicity are necessary to enable the conversion of paper into e-documents to optimize VBMS process and shorten response time to the Veterans. Principles of Purpose Specification, minimization, individual participation, data quality and integrity are ensured by VBA PMCMS through risk assessment strategies including:

Privacy Risk: PMCMS collects PII/PHI/SPI. Due to the sensitive nature of this data, there is a risk that if the data were accessed by an unauthorized individual or otherwise reached, serious harm may result for the individuals affected.

Mitigation: Electronic data is carried in a virtual private network (VPN) that utilizes industry standard technology and encryption algorithms (e.g., AES-256). VBA PMCMS CM Portal is rated as Moderate impact system, in accordance with the Federal Information Processing Standards (FIPS)-

199. All data elements processed and shared are specified by the VBA. As required by the contract, all data is treated as Sensitive (since it consists of a significant volume of PHI, PII, and SPI). Information is transmitted via the VBA's Business Partner Extranet (BPE).

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.

Additional SPI processed includes the VA File number; spouse's Social Security Number (SSN); service-related disabilities; service information; retired/severance pay/pension information; marital and dependency information; income information; and medical and legal expenses necessary to establish, develop, decide, and pay Veteran's claim. VBA PMCMS collects, scans, and disseminates to VBMS and maintains the following data for benefits claims adjudication and processing:

- Veteran File ID Number – information is collected for benefits claimant identification and routing)
- Veteran First Name - – information is collected for benefits claimant identification and routing)
- Veteran Middle Initial - – information is collected for benefits claimant

identification and routing)
- Veteran Last Name - – information is collected for benefits claimant identification and routing)
- Veteran Mailing Address Zip Code - – information is collected for benefits claimant identification and routing)

The following data is not stored as distinct data elements, but the information may appear on scanned document images that are transmitted from the CM Portal to VBMS:

- Veteran SSN
- Veteran DoB
- Mailing address
- Zip code
- Phone number
- Fax number
- Email address
- Emergency contact information
- Health insurance beneficiary info
- Current medication
- Medical history
- Race/ethnicity

Data collected is necessary to establish, develop, decide, and pay a Veteran's claim. It directly supports the VA's VBA VBMS, a paperless claims system that greatly reduces the time required to process a case. The data is used only in support of the business purpose and according to contract stipulations, it is not used for any other purpose.

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

VBA PMCMS does not create new information; scan vendors convert analog data to digital data and then submit that data to CM Portal. That data may be manipulated in a variety of ways but is not transformed. Likewise, the data are not analyzed outside the scope defined by the contract requirements. Tools such as Prometheus and Grafana are used to determine the efficiency of the system, rather than the efficacy of the data.

2.3 How is the information in the system secured?

2.3a What measures are in place to protect data in transit and at rest?

The following table summarizes the Centralized Mail Portal (CMP) communication points with external entities and the encryption methods:

From	To	Service/Protocol	Encryption	Notes
VA Scanning Vendors	CMP Ingest SFTP Servers	sftp	OpenSSH	Vendors access the sftp system using ssh keypairs; FIPS 140-2 Validated SFTP Transfer is required; simple passwords are not used; Port access to TCP 22 is firewalled to only allow vendors and support team access.
CMP/DU Users	CMP UI	https	TLS 1.2	User access is via https with a web browser. Users authenticate using a VA PIV card or ID.Me
CMP Ingest System	VA VBMS	https	TLS/IPSec Tunnel	For INT/UAT access is over TLS to VBMS webserver URL. For PreProd and Prod access is also over TLS to VBMS webserver URL but carried over a private IPSec tunnel directly to the VA internal network.
CMP Ingest System	DU Processing Vendor	sftp	OpenSSH	Vendors access the sftp system using ssh keypairs; simple passwords are not used; Port access to TCP 22 is firewalled to only allow vendors and support team access.
CMP Support Team	CMP Environment Bastion Servers	ssh	OpenSSH	Uses ssh keypairs - simple passwords are not used. Port access to TCP 22 i.e., firewalled to allow only expected IP addresses.
CMP Support Team	AWS Console UI	https	TLS 1.2	MFA is also required for all CMP environments.

CMP Support Team	AWS CLI	ssh	OpenSSH	AWS CLI operations are only permitted via the Bastion or other EC2 instances internal to the environment.

The following table summarized the Centralized Mail Portal (CMP) data storage methods and encryption:

Storage System	Encryption	Notes
S3	Amazon S3 master-key (SSE-S3) AES-256	The scanned PDF images submitted by the vendors are stored in S3 using Server-Side Encryption (SSE). https://aws.amazon.com/s3/faqs/ https://docs.aws.amazon.com/AmazonS3/latest/userguide/security-best-practices.html
EC2 EBS	AES-256	EC2 instances utilize encrypted EBS disk volumes. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html
RDS - SQL	AES-256	The CMP system data stored in PostgreSQL using AWS RDS with storage encryption enabled. https://aws.amazon.com/rds/features/security/

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

There are no additional protections in place for SSNs in the Centralized Mail Portal system. SSNs are treated like all the other PII that the system handles.

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

PMCMS utilizes FedRamp approved Amazon Web Services (AWS). Data is transmitted to VBMS via VA maintained S2S connection over an encrypted tunnel.

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

2.4 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:

Principles of Transparency and Use Limitation are met by VBA PMCMS by ensuring that all data collected, processed, transmitted, and stored by VBA PMCMS is treated as Sensitive. All persons associated with system operation receive initial entry, annual refresher, and ad hoc training on privacy, including Privacy Act, Health Insurance Portability and Accountability Act (HIPAA), system/data security, and the VA Rules of Behavior (RoB). The production personnel process the paper records, any user access to the Information System (IS) is based on what is necessary to do their job. Users are limited to the data needed to track the work and shipments. Administrators are provided access to manage the IS. The VBA PMCMS access control system includes role-based access control (RBAC), based on the following:

- For logical access control, a Windows Active Directory Domain Services (AD DS) model;
- For physical access control, proximity badge-controlled interior and exterior ingress and egress points.

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

All information is only retained to meet contractual business purposes, namely: Name; Social Security Numbers; Date of Birth; Mailing address; Zip Code; Phone Number(s); Fax Number; Email Address; Emergency Contact Information (Name, Phone Number, etc. of a different individual);

Health Insurance Beneficiary Numbers, Certificate/License numbers; Current Medications: Previous Medical Records; and Race/Ethnicity.

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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.

The PMCMS CM Portal retains packet and packet history data for the length of the contract per the VA Business Requirements Document (BRD) specifications. All PDF images are viewable in the CM Portal for a minimum of one (1) year retention period following the date of mail packet completion by VA.

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.

Yes, the system data retention schedule is specified and complies with the base contract, and any changes specified in the Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU). Information contained in the system is restricted to minimum required to meet system objectives. The permanent data records are retained in accordance with the NARA General Records Schedule (GRS) and VBA's Records Control Schedule (RCS) VB-1 and VB-2 (see: https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc and www.benefits.va.gov/WARMS/docs/regs/RCS_II.doc).

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

No Veteran's records are destroyed by SMS/Leidos. At the conclusion of the contract, SMS/Leidos has a Transition Out Plan that details the procedures for decommissioning the system and transferring all data to the VA.

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

This control is inherited from the VA. PMCMS does not determine nor control the use of PII for the purposes of research, testing, nor training. PMCMS only uses PII in accordance with our contract requirements to convert provided paper documents to e-documents. No data, PHI nor PII, is used outside of the scope of the contracted requirements.

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: Operation of VBA PMCMS incurs the standard risks associated with sensitive records management and automated data processing. The possibility of data disclosure occurs during shipment to/from the scan vendor processing facility and during conversion operations or from being retained longer than intended.

Mitigation: The VBA has taken steps to mitigate the possibility of inappropriate data disclosure:

- The project retains only the information necessary for its purpose, only for as long as necessary.
- Internal administration documents used to process, PII/PHI that is no longer needed is returned to secure storage or destroyed.
- Hardcopy data is transported by trusted couriers (USPS, UPS, etc.).
- Electronic data is transmitted and stored only on encrypted media.
- All processing takes place in an accredited secure operations facility.
- PMCMS follows RCS VB-1 and VB-2, as stated in 3.3

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VBMS	To enhance VBMS access to Veteran Data	Name, SSN, DoB, mailing address, zip code, phone number, fax number, email address, emergency contact information, health insurance beneficiary info, current medication, medical history, race/ethnicity.	Dedicated connection with data uploaded via sFTP web services

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: VBA PMCMS could inappropriately use or disclose information, either intentionally or unintentionally.

Mitigation: Extensive physical and logical controls are in place to protect source materials and electronic data. These controls include but are not limited to:

- Facility access control system which uses proximity cards to restrict individual access to their specific areas based upon role.
- Physical controls and procedures which limit the individuals with access to source materials based upon role. Included in these procedures are color coded clip boards and lanyards which are visible and monitored via the building surveillance system.
- Physical facility controls which prevent mobile devices, cameras, purses, bags and other items that could be used to remove confidential materials from entering the production facility.
- Access to the VBA PMCMS is restricted to locked down Citrix sessions which prevents information being copied to removable devices, transmission via email, access to internet- based transmission and the ability to perform screen shots.
- All materials processed through production facilities have chain of custody established via scan vendor records tracking system(s) which identifies the location of the data and who has handled it.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A				

Not Applicable as no information is shared outside of VBMS, the data is not used for any other purpose by PMCMS.

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 - The interconnection from PMCMS DMHS to VBMS is a one-way path. PMCMS CM Portal can connect to VBMS servers, and VBMS can respond to the connection requests. However, VBMS cannot connect back to CM Portal services to access information.

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.

Notice is provided by VBA-Compensation, Pension, Education, and Vocational Rehab and Employment Records via the VBA Systems of Records Notice (SORN) # 58VA21/22/28 and this PIA. This is inherited from and handled by the VA. PMCMS only processes and stores data at the direction of VBMS, the data is not used for any other purpose.

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

Veterans have the right to refuse to disclose their SSNs to VBA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VBA an SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(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

All requests follow VA request channels, must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VBA address outlined within the SORN 58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records. The administration of these requests is done by the VA and those requests are passed from the VA to PMCMS, not directly from any individuals to PMCMS. All information PMCMS receives comes directly at VA direction and it is up to VA to determine whether individuals can consent to particular uses of their information.

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

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

<u>Principle of Use Limitation:</u> Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:
Privacy Risk: The individual may not be aware of published notice(s).

Mitigation: This PIA and the published SORN serves to notify Veterans about the collection, use, and storage of personal information. Notice, access, redress, and correction would be handled via the standard VA request channels for change. Their information is held in PMCMS only to provide enhanced access to VBMS, it is not used for any other purposes by PMCMS.

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.

Veterans may request access to Privacy Act records maintained by requesting a copy in writing. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VBA system of records, the facility Privacy Officer, or their designee.

Each request must be date stamped and reviewed to determine whether the request for access should be granted. This is inherited from and handled by the VA, it is outside the scope of this contract, and not administered by PMCMS.

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

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

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

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The procedure for correcting information is outlined above. Formal redress is provided. All information correction must be taken via the Amendment process. This is handled by the VA, it is outside the scope of this contract, and not administered by PMCMS.

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 ensures data accuracy.

Formal redress is provided. All information correction must be taken via the Amendment process. This is inherited from and handled by the VA, it is outside the scope of this contract for administration by PMCMS.

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: There is a risk that incorrect information is accidentally recorded in an individual's record.

Mitigation: PMCMS scan vendors have controls and processes in place to ensure that documents from one individual do not mistakenly get mixed into those from another individual. These controls and processes are documented and maintained by the scan vendor(s) and are outside of the scope for PMCMS CM Portal. CM Portal does offer authorized users the ability to correct the following details within a veteran's packet:

- Veteran File Number
- Veteran First Name
- Veteran Middle Initial
- Veteran Last Name
- Emergent Flashes

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 control is maintained in accordance with FIPS Publication 199 *Moderate* information system control standards. SMS/Leidos follows the Principle of Least Privilege when approving access to any system and/or data. System users and administrators are given only the minimum access necessary to perform their function(s). Standard minimum access profiles are maintained via security groups for all logical and physical access. Role-based access requests and revocations are forwarded to the Network Infrastructure and Security teams by operations supervisors, as part of the onboarding, change of information, and termination processes.

Example roles with system/data access include those shown below. All are carefully analyzed, to ensure that only the minimum required access is allowed:

- Administrator (Domain, Enterprise, Organizational Unit (OU))
- Chief Information Officer
- Chief Information Security Officer
- Chief Technology Officer
- Computer Systems Operator (Help Desk)
- Computer Support Specialist (Help Desk)
- Data Capture Operator (Operations)
- Document Processor (Operations)
- Driver (Operations)
- Facilities Administrator (Operations)
- Media Processor (Operations)
- Operations Manager (Operations)
- Processor (Operations)
- Project Support Specialist
- Quality Assurance Analyst (Operations)
- Records Center Associate
- Scanner Operator (Operations)
- Security Engineer
- Software Engineer
- Supervisor (Operations)
- Systems Analyst
- Team Lead (Operations)
- Vice President – Application Development
- Vice President – Client Services
- Vice President – Network Infrastructure Technology

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

VBA PMCMS is a contractor-furnished and maintained system; a VA security clearance is required for all persons having access to systems and/or data. Ongoing training is maintained, and ROB and NDA are signed.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All persons associated with VBA PMCMS development, operation, and maintenance receive initial entry, annual refresher, and ad hoc training on privacy, including the Privacy Act, HIPAA, system and data security, and the VA Rules of Behavior.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *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.***

Authorization to Operate (ATO) VBA PMCMS, A FIPS Publication 199 Moderate system, was last granted conditionally on 07 January 2022 for three years.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

The Centralized Mail Portal (CMP) component of the PMCMS system uses Amazon Web Services (AWS) Govcloud. AWS Govcloud offers FedRAMP compliant services.

Is Amazon Web Services FedRAMP compliant?

Yes, AWS offers the following FedRAMP compliant services that have been granted authorizations, have addressed the FedRAMP security controls (based on NIST SP 800-53), used the required FedRAMP templates for the security packages posted in the secure FedRAMP Repository, has been assessed by an accredited independent third party assessor (3PAO) and maintains continuous monitoring requirements of FedRAMP:

- **AWS GovCloud** (US), has been granted a Joint Authorization Board Provisional Authority-To- Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for high impact level. The services in scope of the AWS GovCloud (US) JAB P-ATO boundary at high baseline security categorization can be found within **AWS Services in Scope by Compliance Program.**
- **AWS US East-West** (Northern Virginia, Ohio, Oregon, Northern California) has been granted a Joint Authorization Board Provisional Authority-To- Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for moderate impact level. The services in scope of the AWS US East-West JAB P-ATO boundary at Moderate baseline security categorization can be found within **AWS Services in Scope by Compliance Program.**

Source: https://aws.amazon.com/compliance/fedramp/

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

AWS policy is that the customer accounts own and maintain sole control of all data in the service account (https://aws.amazon.com/compliance/data-privacy/).

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

AWS collects ancillary data for the purposes of auditing activities and billing for service usage. Presumably AWS owns this data to use for its business purposes.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Per AWS documentation, the customers own and are responsible for controlling and securing the data stored in the cloud account.

- **Access:** As a customer, you maintain full control of your content that you upload to the AWS services under your AWS account, and responsibility for configuring access to AWS services and resources. We provide an advanced set of access, encryption, and logging features to help you do this effectively (e.g., **AWS Identity and Access Management, AWS Organizations** and **AWS CloudTrail**). We provide APIs for you to configure access control permissions for any of the services you develop or deploy in an AWS environment. We do not access or use your content for any purpose without your agreement. We never use your content or derive information from it for marketing or advertising purposes.
- **Storage:** You choose the AWS Region(s) in which your content is stored. You can replicate and back up your content in more than one AWS Region. We will not move or replicate your content outside of your chosen AWS Region(s) without your agreement, except as necessary to comply with the law or a binding order of a governmental body.
- **Security:** You choose how your content is secured. We offer you industry-leading encryption features to protect your content in transit and at rest, and we provide you with the option to manage your own encryption keys. These data protection features include:
  - **Data encryption capabilities available in over 100 AWS services.**
  - **Flexible key management options using AWS Key Management Service (KMS)**, allowing customers to choose whether to have AWS manage their encryption keys or enabling customers to keep complete control over their keys.
- **Disclosure of customer content:** We will not disclose customer content unless we're required to do so to comply with the law or a binding order of a government body. If a governmental body sends AWS a demand for customer content, we will attempt to redirect the governmental body to request that data directly from the customer. If compelled to disclose customer content to a government body, we will give customers reasonable notice of the demand to allow the customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so.
- **Security Assurance:** We have developed a security assurance program that uses best practices for global privacy and data protection to help you operate securely within AWS, and to make the best use of our security control environment. These security protections and control processes are independently validated by **multiple third-party independent assessments.**

Source: https://aws.amazon.com/compliance/data-privacy-faq/

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

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

The CMP component of the PMCMS system does not use any RPA to manipulate the customer packet data containing PII/PHI maintained in the system.

PMCMS does use automated scripts and programs for the following system level purposes that do not directly manipulate PII/PHI:

- System backups
- Report generation regarding system data and status for project tracking.
- System performance monitoring and alerting for problems and errors.

- System controls and automatic scaling operations.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

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.

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2022.07.08 07:03:41 -06'00'

Privacy Officer, Jean-Claude Wicks

RICHARD ALOMAR-LOUBRIEL 139039

Digitally signed by RICHARD ALOMAR-LOUBRIEL 139039
Date: 2022.07.11 07:05:50 -04'00'

Information System Security Officer, Richard Alomar-Loubriel

DEREK HERBERT

Digitally signed by DEREK HERBERT
Date: 2022.07.08 10:31:47 -04'00'

Information System Owner, Derek Herbert

APPENDIX A-6.1

https://www.federalregister.gov/documents/2019/02/14/2019-02315/privacy-act-of-1974-system-of-records