Privacy Impact Assessment for the VA IT System called:

Delivery Operations Claims Management Platform (DOCMP)

Veterans Health Administration

Office of Integrated Veteran Care (IVC)

eMASS ID #2003

Date PIA submitted for review:

April 10, 2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Eller Pamintuan	eller.pamintuan@va.gov	(303) 331-7512
Information System Security Officer (ISSO)	Amine Messaoudi	Amine.messaoudi@va.gov	(202)815-9345
Information System Owner	Jeffrey Rabinowitz	Jeffrey.rabinowitz@va.gov	(732)720-5711

Abstract

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

The Delivery Operations Claims Management Platform (DOCMP) is a suite of claim processing components and related applications within Office of Integrated Veteran Care (IVC) supporting claims processing systems. This platform assists with determination of eligibility for Civilian Health and Medical Program of the Department of Veterans Affairs (CHAMPVA) programs, adjudication of claims and appeals, and creation, management, and printing of denial letters. In addition to the business rule process, these components enable creation of reports to assist several teams in pulling transactional information as it relates to the workflow processes supported in DOCMP.

Overview

The overview is the most important section of the Privacy Impact Assessment (PIA). A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

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

The Delivery Operations Claims Management Platform (DOCMP) receives patient data and documentation from sources including clinical, administrative, and financial information systems, other Electronic Health Record (EHR) systems, Personal Health Record (PHR) systems, and data received through health information exchange networks.

DOCMP collects the information to assist with determination of eligibility for Civilian Health and Medical Program of the Department of Veterans Affairs (CHAMPVA) programs, adjudication of claims and appeals, and creation, management, and printing of denial letters. In addition to the business rule process, these components enable creation of reports to assist several teams in pulling necessary information as it relates to all aspects of claims including cost, eligibility, and payment data.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

VA owned and VA Operated

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

3.6 million Veterans and Family Members

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☐	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☒	Members of the Public/Individuals
☐	Volunteers

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

DOCMP receives patient data and documentation from sources including clinical, administrative, and financial information systems, other Electronic Health Record (EHR) systems, Personal Health Record (PHR) systems, and data received through health information exchange networks.

DOCMP collects the data to assist with determination of eligibility for CHAMPVA programs, adjudication of claims and appeals, and creation, management, and printing of denial letters. In addition to the business rule process, In addition to the business rule process, these components enable creation of reports to assist several teams in pulling transactional information as it relates to the workflow processes supported in DOCMP.

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

DOCMP is a processing application for CHAMPVA and Foreign Medical Program (FMP), including all supplementary forms and documentation; appeals documentation; FMP paper claims; and 8-point denial letters and related records. Information is shared as identified in Section 4.1 and Section 5.1. Data is encrypted in transit.

F. Are the modules/subsystems only applicable if information is shared?

Yes, all data elements are shared with internal DOCMP modules.

G. Is the system operated in more than one site to include primary and secondary 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?

DOCMP operates in the in the Enterprise Cloud (VAEC) Amazon Web Services (AWS) Government.

Backup data durability is obtained by synchronously replicating data in the alternate site.

3. Legal Authority and System of Record Notices (SORN)

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

- Legal Authority: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.
- Legal Authority: Title 38, United States Code, Sections 501(b) and 304.
- Legal Authority: 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.
- Legal Authority: Title 38, United States Code, section 7301(a).
- Legal Authority: 31 U.S.C. 3101 and 31 U.S.C. 3102. The purpose of the system is consistent with the financial management provisions of title 31, United States Code, chapter 37, the pay administration provisions of title 5, United States Code, chapter 55, and special provisions relating to VA benefits in title 38, United States Code, chapter 53.
- Legal Authority: Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317

H. What is the SORN?

- *23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015), https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf*
- *24VA10A7, Patient Medical Records - VA (10-2-2020), https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf*
- *54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015), https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf*
- *79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf*
- *88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13/2018), https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf*
- *147VA10, Enrollment and Eligibility Records - VA (8-17-2021), https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf*

I. SORN revisions/modification

Per the PTA guidance SORNs must be updated if older than 6 years from date of publication in the Federal Register. SORNs 23VA10NB3 and 54VA10NB3 are currently under revision as they are over 6 yrs old.

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

No modifications are needed for the SORNs

4. System Changes

J. *Will the business processes change due to the information collection and sharing?*

☒ *Yes*
☐ *No*
if yes, The users no longer need to print and scan all documents. Denial letters were manually created in the past and now the letter creation process will be automated by sending the print files to an external print vendor.

K. *Will the technology changes impact information collection and sharing?*

☐ *Yes*
☒ *No*
if yes, <<ADD ANSWER HERE>>

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 Information collected, used, disseminated, created, or maintained in the system.

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name

☒ **Full** Social Security Number
☒ **Partial** Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Information

☒ Health Insurance Beneficiary Numbers Account Numbers
☒ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☒ Medical Records
☐ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☐ Sex
☒ Integrated Control Number (ICN)

☐ Military History/Service Connection
☐ Next of Kin
☐ Date of Death
☐ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (list below)

Other PII/PHI data elements:

- Claim ID #
- Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes
- Date(s) of Service
- File Number
- Healthcare Provider Name
- Insurance Provider Information
- International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)

1.2 List the sources of the information in the system
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Data is sourced from a Veteran or Veteran Beneficiary, but DOCMP does not receive that data directly from an individual. The data is provided to DOCMP via electronic transmission from Veterans-Facing Services Platform VA.GOV(VFSP)/AWS.GOV/VA.GOV, Teleform (Legacy DAPER), Enterprise Cloud Fax (ECFAX) Messenger, Consolidated Intake of and Processing Mail (CIPM), Payer Electronic Data Interchange (EDI) Transactions Applications Suite (TAS)(Payer EDI TAS), and Claims Processing and Eligibility (CP&E).

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

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Veterans-Facing Services Platform VA.GOV(VFSP), AWS.GOV/VA.GOV, Teleform (Legacy DAPER), Enterprise Cloud Fax (ECFAX) Messenger, and Consolidated Intake of and Processing Mail (CIPM) are ways for the veteran for beneficiary to interact with DOCMP. Payer EDI TAS provides automated information on claims for efficiency.

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

The System does not generate scores, analysis, or reports.

1.3 Methods of information collection

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

The data is provided to DOCMP via electronic transmission from Veterans-Facing Services Platform VA.GOV(VFSP)/AWS.GOV/VA.GOV, Teleform (Legacy DAPER), Enterprise Cloud Fax (ECFAX) Messenger, Consolidated Intake of and Processing Mail (CIPM), Payer Electronic Data Interchange (EDI) Transactions Applications Suite (TAS)(Payer EDI TAS), and Claims Processing and Eligibility (CP&E).

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

Information is collected on form 10-10d and for application benefits 10-7959.

1.4 Information checks for accuracy, and how often will it be checked.

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Information is checked at the time of ingestion using a combination of automated and manual checks. Once ingested the data not checked again unless there is notification of a change which needs to be made to the historical data. The forms and or associated documentation images in DOCMP are checked against existing data in IVC VistA. If they do not match,

additional processes are engaged to gather the correct information to process the application. Incorrectly completed forms 10-10d and application benefits 10-7959 are worked by CHAMPVA Staff. Contact would be made with the VistA owner to correct data when appropriate.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

The system does not utilize a commercial aggregator of information to check for accuracy.

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

- SORN: 23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015), https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

  Legal Authority: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.
- SORN: 24VA10A7, Patient Medical Records - VA (10-2-2020), https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

  Legal Authority: Title 38, United States Code, Sections 501(b) and 304.
- SORN: 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015), https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf

  Legal Authority: 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.
- SORN: 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020), https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf
  Legal Authority: Title 38, United States Code, section 7301(a).
- SORN: 88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13/2018), https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

  Legal Authority: 31 U.S.C. 3101 and 31 U.S.C. 3102. The purpose of the system is consistent with the financial management provisions of title 31, United States Code, chapter

37, the pay administration provisions of title 5, United States Code, chapter 55, and special provisions relating to VA benefits in title 38, United States Code, chapter 53.

- SORN: 147VA10, Enrollment and Eligibility Records - VA (8-17-2021), https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

  Legal Authority: Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

Principle of Purpose Specification: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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: Data pulled by the DOCMP application contains PII. If the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft might result.

Mitigation: The DOCMP application ensures strict access to information by enforcing thorough access control and requirements for end users. Access to the application is by PIV authentication. Individual administrator user IDs and access are provided based on need. DOCMP limits access rights and controls only to valid end users. There are rigorous securities monitoring controls to prevent unauthorized access and intrusion, and to protect all information. Furthermore, all end users are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. All users with access to DOCMP are responsible in assuring safeguards for the PII/PHI.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Used to identify Veteran for Beneficiary identification	Used to print denial letters
Full Social Security Number	Used to verify Beneficiary identity and as a file number for the Beneficiary. Used to properly identify patient or provider, adjudicate and pay claims	Not used
Partial Social Security Number	Used to verify Beneficiary identity and as a file number for the Beneficiary. Used to properly identify patient or provider, adjudicate and pay claims	Not used
Date of Birth (DOB)	Identify the patient's age and confirm patient identity. Used for Beneficiary identification	Not used
Personal Mailing Address	Used to verify the correct address	Used to print denial letters
Personal Phone Number(s)	Used to give the pharmacist an easy way to contact the Beneficiary if necessary to clarify pharmacy issues	Not used
Personal Fax Number	Forms are received by fax number. It is inherent	Not used
Personal Email Address	Used to contact patient, to properly identify patient, and adjudicate and pay claims	Not used
Financial Information	Used to Adjudicate and pay claims	Not used
Health Insurance Beneficiary Numbers Account Numbers	Used to identify patient Health Insurance Account Information:	Not used

PII/PHI Data Element	Internal Use	External Use
	Used to view information on claims	
Certificate/License Numbers	Used for external provided credentialing	Not used
Medical Records	Used to cross reference the patients' medical conditions with the pharmacological potential drug side effects	Not used
Tax Identification Number (TIN)	Used to verify Beneficiary identity and as a file number for the Beneficiary. Used to properly identify patient or provider, adjudicate and pay claims	Not used
Medical Record Number	Used to cross reference the patients' medical conditions with the pharmacological potential drug side effects	Not used
Integrated Control Number (ICN)	Used to identify Veteran for Beneficiary identification	Not used
Claim ID #	Used to properly verify the correct claim for payment to adjudicate and pay claims.	Used to print denial letters
Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes	Used to properly verify the correct procedure for payment to adjudicate and pay claims.	Not used
Date(s) of Service	Identify health care information status	Used to print denial letters
File Number	Submitted in documents, such as rating decisions	Not used
Healthcare Provider Name	Used to properly identify the medical provider, adjudicate and pay claims	Used to print denial letters
Insurance Provider Information	Used to properly identify the Insurance provider, adjudicate and pay claims	Not used
International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)	Used to verify correct service for payment to adjudicate and pay claims.	Not used

2.2 Describe the types of tools used to analyze data and what type of data may be produced.

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

Power BI can connect individuals with the appropriate authorization to DOCMP so that users can ask and answer sophisticated questions of their data.

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

DOCMP does not create or make available new or previously unutilized information about an individual. Comments can be added to an existing record as part of the internal workflow process.

2.3 How the information in the system is secured.

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

DOCMP uses either proprietary Oracle encryption for data at rest and IIS/Apache for data in transit. PEGA uses proprietary AWS encryption and firewalls to protect the data within the AWS environment. DOCMP also limits traffic to internal users. Access to PII is provided to those staff that are deemed necessary via ePAS. The VA limits access of PII only to staff as appropriate to their role in Veteran Care.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

DOCMP truncates Social Security Numbers and encrypts data in transit and at rest. The VA limits access of PII only to staff as appropriate to their role in Veteran Care. A limited group of users are granted permission to view SSNs as part of their role. This elevated privilege group has been granted permission through the Electronic Permission Access System (EPAS) upon supervisor’s approval.

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

Users are restricted to transmission within VA Secure network.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Access to PII is limited by the application to only those data items deemed necessary for a stakeholder to perform their job, as determined by their management team and their job description.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

System documentation includes detailed system design and user guides that specify those areas of the system that contain PII and PHI, as well as how it is to be used by the stakeholder. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles within the system are determined and requested by supervisors and Business Implementation Managers. User access is provided by the System Administrators following receipt of request from appropriate individuals. The application implements auditing which tracks user access to the system and all data accessed.

All DOCMP documentation regarding access controls are documented in policy and procedure and/or SOPs documents which are stored within secure SharePoint sites as well as within EMASS

2.4c Does access require manager approval?

Yes, this elevated privilege group is granted permission upon supervisor's approval.

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

The DOCMP system implements auditing which tracks user access to the system and all data accessed. The information is mapped in the audit record. VA Clearance procedures are implemented to monitor access, and accounts are disabled after 30 days of inactivity.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

VHA ensures that the practices stated in the PIA are reinforced by requiring Contractors and VA employees to complete all VA trainings including VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203).

Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply. Through TMS employees and contractors are monitored, CORS are responsible for ensuring assignment in TMS training. Training audits occur monthly and are conducted by ISSOs throughout the VA. Training records are stored in the TMS system. Any user who is not current in Privacy/Infosec training loses access to all VA data (including DOCMP) until they become current on required training. All incidents are required to be reported to the supervisor or ISSO / Privacy Officer within 1 hour of occurrence. If the ISSO determines a security event has occurred, they open a PSETS ticket and inform CSOC and DBRS. Credit monitoring may be provided to any person whose sensitive information has been violated, and the system user who put the data at risk will be retrained and consequences of actions up to loss of job. Privacy Risk: MbM employees may not adhere to the information security requirements instituted by the VA OI&T and the information from the internal web portal may be shared outside the scope of the processing center unintentionally, leaving open the risk of identity theft. Mitigation: VHA ensures that the practices stated in the PIA are reinforced by requiring Contractors and VA employees to complete all VA trainings: VA Privacy and Information Security Awareness and rules of Behavior Training, and Privacy and HIPAA focused training. Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply. For further details, see Section 8: Technical Access and Security. If or when a privacy breach occurs, it is reported to the appropriate privacy officers and when warranted, identifies protection services are offered to the beneficiary.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

- Name
- Full Social Security Number
- Partial Social Security Number
- Date of Birth
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Financial Information
- Health Insurance Beneficiary Numbers Account Numbers
- Certificate/License Numbers
- Medical Records

- Tax Identification Number
- Medical Record Number
- Integrated Control Number (ICN)
- Claim ID #
- Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes
- Date(s) of Service
- File Number
- Healthcare Provider Name
- Insurance Provider Information
- International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

The information/data/records in DOCMP system are purged in accordance with the designated VHA records control schedule as stated in this PIA.

VHA Records Control Schedule (RCS) 10-1, 1260 – Care in Community, Health and Medical Care Program VA

RCS: 1260.1. Civilian Health and Medical Care (CHMC) Records.

a. Unscanned Records. All documents maintained in paper form. Temporary; destroy 6 years after all individuals in the record become ineligible for program benefits. (N1-15-03-1, item 1)

b. Input Scanned Records. Paper source documents that have been scanned for electronic media storage (optical disk). Temporary; destroy after successfully scanned to electronic medium. (N1-15-03-1, item 2)

c. Electronic Records (Master Files). Electronic records produced form scanned documents or records received electronically (optical disk, magnetic tape, or another electronic medium). Temporary; destroy 6 years after all individuals in the record become ineligible for program benefits. (N1-15-03-1, item 3)

A Backup Plan and Restore Plan were developed and implemented using industry best practices. At a minimum, the plan includes the requirement to save data for the backup and recovery of information stored on the storage infrastructure to meet related Service Level

Agreements (SLAs), and the retention of records as required by VA Handbook 6300.1 (Records Management Procedures) and VA Directive 6300 (Records and Information Management). Backups are conducted on a daily/weekly basis. The DOCMP system retains funding records 6 years after all individuals in the record become ineligible for program benefits.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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

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

Yes

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

VHA Records Control Schedule (RCS) 10-1 (http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf)
VHA Records Control Schedule (RCS) 10-1, 1260 – Care in Community, Health and Medical Care Program VA (http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf)
RCS: 1260.1. Civilian Health and Medical Care (CHMC) Records.

a. Unscanned Records. All documents maintained in paper form. Temporary; destroy 6 years after all individuals in the record become ineligible for program benefits. (N1-15-03-1, item 1)
b. Input Scanned Records. Paper source documents that have been scanned for electronic media storage (optical disk). Temporary; destroy after successfully scanned to electronic medium. (N1-15-03-1, item 2)
c. Electronic Records (Master Files). Electronic records produced form scanned documents or records received electronically (optical disk, magnetic tape, or another electronic medium). Temporary; destroy 6 years after all individuals in the record become ineligible for program benefits. (N1-15-03-1, item 3)

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the Deleted Items or Recycle bin. Magnetic media is wiped and sent out for

destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1 and NIST SP800-88r1 as evidenced in the FedRAMP Audit reports.

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

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

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

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training, and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

No, this is a production system.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of

PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe policies and procedures for how PII that is no longer relevant and necessary is purged.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk:

There is a risk that the information maintained by DOCMP could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk of retained information being breached, DOCMP adheres to the VA RCS schedules, all data is destroyed 6 years after all individuals in the record become ineligible for program benefits. reporting.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **DOCMP** consists of **12** key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **DOCMP** and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
DOCMP Workflow Tool DAPER PEGA prod db	**Yes**	**Yes**	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number	Eligibility, Appeals processing, and Foreign paper claims processing.	System is internal to VA. Only approved employees and contractors have access to the system.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)		
DOCMP Workflow Tool DAPER PEGA prod db cluster	**Yes**	**Yes**	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID #	Eligibility, Appeals processing, and Foreign paper claims processing.	System is internal to VA. Only approved employees and contractors have access to the system.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)		
DOCMP Workflow Tool PEGA	**Yes**	**Yes**	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers	Eligibility, Appeals processing, and Foreign paper claims processing	System is internal to VA. Only approved employees and contractors have access to the system.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)		
AWS S3 Bucket: AWS S3 Bucket (VA.GOV) AWS S3 Bucket (CIPM) AWS S3 Bucket (DAPER) AWS S3 Bucket (Processed) AWS S3 Bucket (PEGA)	**Yes**	**Yes**	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s)	Eligibility, Appeals processing, and Foreign paper claims processing.	System is internal to VA. Only approved employees and contractors have access

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)		to the system.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
AWS Lambda - PEGA	**Yes**	**Yes**	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number	Eligibility, Appeals processing, and Foreign paper claims processing.	System is internal to VA. Only approved employees and contractors have access to the system.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)		
AWS API Gateway - PEGA	**Yes**	**Yes**	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID #	Eligibility, Appeals processing, and Foreign paper claims processing.	System is internal to VA. Only approved employees and contractors have access to the system.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)		
AWS Data Sync Agent	**Yes**	**Yes**	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers	Eligibility, Appeals processing, and Foreign paper claims processing.	System is internal to VA. Only approved employees and contractors have access to the system.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)		
AWS S3 Buckets (8PDL) (8):	**Yes**	**Yes**	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s)	Printing of Denial letters	System is internal to VA. Only approved employees and contractors have access

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)		to the system.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
8 Point Denial database (Oracle)	**Yes**	**Yes**	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number	Printing of Denial letters	System is internal to VA. Only approved employees and contractors have access to the system.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)		
8 Point Denial 8PDL Audit DB (Oracle)	**Yes**	**Yes**	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID #	Printing of Denial letters	System is internal to VA. Only approved employees and contractors have access to the system.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)		
8 Point Denial Web/application server	**Yes**	**Yes**	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers	Printing of Denial letters	System is internal to VA. Only approved employees and contractors have access to the system.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)		
ODM Operational Decision Manager (ODM)	**Yes**	**Yes**	Full Social Security Number	Process Foreign Medical claims and Appeals	

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Payer EDI TAS	Denials Letter creation	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology	s3-s3 communication

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		(CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)	
VETERANS-FACING SERVICES PLATFORM VA.GOV(VFSP) AWS.GOV/VA.GOV	Determine eligibility for claims processing	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision,	s3-s3 communication

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		Clinical Modification Codes (ICD-10-CM)Certificate/License Numbers	
Appeals	Process Appeals	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)	SMB Connection
Teleform (Legacy DAPER)	Determine eligibility for claims processing	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address	AWS Data Sync

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)	
Enterprise Cloud Fax (ECFAX) Messenger	Determine eligibility for claims processing	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number	AWS Data Sync

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)	
Claims Processing and Eligibility CP&E	Process Foreign Medical claims and Appeals	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name	Via SOAP and Secure File Transfer Protocol (SFTP)

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		Insurance Provider Information International Classification of Diseases, Tenth Revision, Clinical Modification Codes (ICD-10-CM)	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: Disclosure of information from a third party.

Mitigation: An Interconnection Security Agreement / Memorandum of Understanding (ISA/MOU) defining the system and data transmission in is in place. Access to the data is limited to appropriate personnel who are required to be trained in the handling of VA PII/PHI and sensitive information.

Privacy Risk: Privacy information may be inadvertently released to unauthorized individuals or the source applications (i.e., Payer EDI, VFSP VA.gov, Appeals, Teleform (Legacy DAPER), ECFAX , and CP&E) with which the application interfaces with may inadvertently release privacy information. If such an instance should occur the impact is considered low..

Mitigation: The application ensures strict access to information by enforcing through access control and requirements for end users. Access to the application is by PIV authentication. Individual administrator user IDs and access are provided only based on need. The application limits access rights and controls only to valid end users. Rigorous security monitoring controls are in place to prevent unauthorized access and intrusion, and to protect all information. Furthermore, all end users are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. The VA IT office is responsible in assuring safeguards for the PII.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Kessler Creative (Print Vendor) Denial Letter printing	Printing of denial letters	Name Personal Mailing Address Claim ID # Current Procedural Terminology (CPT)/Healthcare	MOU/ISA	Secure File Transfer Protocol (SFTP) / Data encrypted in transfer

List IT System or External Program Office information is shared/received with	*List the purpose of information being shared / received / transmitted*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)*	*List the method of transmission and the measures in place to secure data*
		Common Procedure Coding System (HCPCS) Codes Date(s) of Service Healthcare Provider Name Insurance Provider Information		
Consolidated Intake of and Processing Mail (CIPM)	Determine eligibility for claims processing	Name Full Social Security Number Partial Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Fax Number Personal Email Address Financial Information Health Insurance Beneficiary Numbers Account Numbers Certificate/License Numbers Medical Records Tax Identification Number Medical Record Number Integrated Control Number (ICN) Claim ID # Current Procedural Terminology (CPT)/Healthcare Common Procedure Coding System (HCPCS) Codes Date(s) of Service File Number Healthcare Provider Name Insurance Provider Information International Classification of Diseases, Tenth Revision,	MOU/ISA	s3-s3 communication / Data encrypted in transfer

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
		Clinical Modification Codes (ICD-10-CM)		

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: There is a risk that PII/PHI may be accidently released to unauthorized individuals.

Mitigation: Memorandum of Understanding / Interconnection Security Agreement (MOU/ISA) agreements are in place ensuring the proper processes are in place to prevent disclosure of PII/PHI. The entity must provide the minimum necessary policies and procedures, or a secure alternative to the extent consistent with the VA policies and procedures and must comply with the HIPAA Privacy rules.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

It is Veterans Health Administration (VHA) policy that the VHA Notice of Privacy Practices (Information Bulletin 10-163) is created, maintained, and distributed in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule at 45 C.F.R. § 164.520, to inform Veterans, beneficiaries, caregivers, and non-Veteran patients of the use and disclosure of their health information without authorization, their rights to access and restrictions on certain uses and disclosures and VHA's legal duties to maintain the privacy of their health information. **AUTHORITY:** 45 C.F.R. parts 160 and 164. VHA Notice of Privacy Practice https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

This Privacy Impact Assessment (PIA) also serves as notice of the DOCMP system. As required by the eGovernment Act of 2002, Pub.L. 107-334 §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." https://department.va.gov/privacy/privacy-impact-assessments/

System of Record Notices (SORNs) - The Privacy Act requires agencies to "publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records" subject to the Act (5 U.S.C. 552a(e)(4)).

23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015);
https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

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

54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015);
https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020); https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13/2018); https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

147VA10, Enrollment and Eligibility Records - VA (8-17-2021); https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

6.1b If notice was not provided, explain why.

N/A. Notice was provided.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Notice is provided via the publication of this PIA at https://department.va.gov/privacy/privacy-impact-assessments/

Notice is provided via VHA Privacy Notice: https://www.oprm.va.gov/privacy/about_privacy.aspx upon enrollment to the VFMP and FMP programs.

SORNS

https://department.va.gov/privacy/system-of-records-notices/

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

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

VHA Directive 1605.1, Privacy and Release of Information, paragraph 5, lists the Individuals' Rights of the Veterans and Beneficiaries to request VHA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. Veterans have the right to refuse to disclose their SSNs to VHA. The individual is denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (please refer to the: 38 Code of Federal Regulations CFR 1.575(a)).

If the Veterans or Beneficiaries does not wish to provide their SSN, they may provide their EDIPI. Alternatively, they may provide their First Name, Last Name, and Date of Birth. If the stakeholder does not wish to provide any of this information, there is no denial of service; however, the employee will be unable to assist the stakeholder.

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

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

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

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 employees do not provide notice to stakeholders, then they will not know how the information they provide to the application is being used. The magnitude of impact is low if Veterans and Beneficiaries are not provided this notice because the employees are not collecting new data. The employees are merely verifying authoritative data stored in MPI, E&E, HDR, and CP&E.

Mitigation: Contractor and VA employees are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. In addition, this PIA, which will be available online as required by the eGovernment Act of 2002, Pub. L. 107–347§208(b)(1)(B)(iii), serves to notify Veterans, Beneficiaries and Providers about the collection and storage of personal information.

Privacy Risk: Privacy Information is used or disclosed outside of its intended purpose.

Mitigation: This PIA serves to notify Veterans and Beneficiaries about the collection and storage of personal information.
1. Beneficiaries are provided notice of Privacy Practices upon enrollment.
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's website at https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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 The procedures that allow individuals to gain access to their information.

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

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

VHA Directive 1605.01: Privacy and Release of Information states the rights of Veterans and Beneficiaries to request access to review their records. VA Form 10-5345a, *Individual's Request for a Copy of Their Own Health Information*, may be used as the written request requirement. All requests to review or seek copies of records must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access to data must be delivered to, and reviewed by, the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must include the signature of the requester, date of birth, copy of signed government identification, state what is request and the period of the information requested. Mail requests for eligibility information/records to: CHAMPVA Eligibility PO Box 137, Spring City, PA 19475. Mail requests for CHAMPVA billing/claim records to: VHA Office of Integrated Veteran Care Privacy/FOIA Office, PO Box PO Box 137, Spring City, PA 19475. Requests for medical and pharmacy records contact your servicing medical provider and for Community Care authorizations/authorization numbers are located at the referring VA Medical Center. For Veteran claim payment information will need to be submitted to the VA Financial Services Center (FSC) Privacy Office by first contacting them via email at vafscprivacyofficer@va.gov for secure submission methods. For Veteran Explanation of Benefits maintained by the VA's Third-Party Administrators may be requested by the Veteran registering and requesting their records from either (TriWest Healthcare Alliance) (https://veteran.triwest.com/bizflowappdev/apps/veteranportal/?tz=GMT-0700 or Optum (https://veteran.vacommunitycare.com/start). Medical and pharmacy records should be sought from the medical facility where the patient received care and Veteran and Beneficiary (CHAMPVA) lien or subrogation requests should be submitted to the respective action office via the instructions located at https://www.va.gov/OGC/Collections.asp. Additionally, a link to the VA Notice of Privacy Practices is provided at Appendix A.

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

This system is not exempt from the access provisions of the Privacy Act.

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

The system is a Privacy Act System.

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

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

The Veterans and Beneficiaries may request changes to their information in accordance with VHA Directive 1605.01, Privacy and Release of Information, paragraph 5, paragraph 8 states the rights of Beneficiaries to amend their records by submitting a written request. This includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request must be mailed and routed to the Office of Integrated Veteran Care Privacy/FOIA Office, PO Box 700, Spring City, PA 19475 , to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579..

7.3 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.

Individuals are informed of the amendment process by many resources to include:

- VHA Privacy Notice: https://department.va.gov/privacy/va-privacy-policies/
- VA Privacy Impact Assessment: https://www.oprm.va.gov/privacy/pia.aspx
- VHA Systems of Records Notice: https://department.va.gov/privacy/system-of-records-notices/

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or

group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Formal redress is provided.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

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

Mitigation: An individual who wishes to determine whether a record is being maintained in this system under their name or other personal identifier, or who wants to review the contents of such a record, should submit a written request to the Office of Integrated Veteran Care Privacy/FOIA Office, PO Box 700, Spring City, PA 19475, to be date stamped; and is filed appropriately. Inquiries should include the patient's full name, SSN, and return address.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

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

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

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

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

Access is limited to VA Contractors and VA employees. No outside agencies.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Standard User – Read-Only data, Add comments to records;
Supervisor - Approves Access requests and performs semi-annual reviews
Privileged – Administers and maintains DOCMP system.

8.2a. Will VA contractors have access to the system and the PII?

Yes.

DOCMP development contractors design and build DOCMP and continue to update and maintain the system.

CIPM contractors scan documents that contain PII.

Kessler Creative contractors receive print files, print, and mail denial letters. The denial letters contain PII.

8.2b. What involvement will contractors have with the design and maintenance of the system?
Contractors designed and built DOCMP and continue to update and maintain the system.

8.2c. Does the contractor have a signed confidentiality agreement?

Yes.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

DOCMP development contractors have implemented Business Associate Agreements.

External Contractors are responsible for establishing and maintaining Business Associate Agreements. This information is covered in the MOU/ISA for GDIT/CIPM, and Kessler Creative**.**

8.2e. Does the contractor have a signed non-Disclosure Agreement in place? Yes.
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.

DOCMP development contractors are limited with access to production to those necessary to support said architecture. The only exposure to PHI/PII is during testing for production or when necessary for production configuration. Developers, for example, do not have access to production and as such do not have access to PHI/PII.

Contractors must have successfully completed VA contractor background security investigation as per the Position Designation Automated Tool (PDT).

The Contracting Officer Representative (COR) is responsible for ensuring that all contractors who are working on the DOCMP project have signed Non-Disclosure Agreements and necessary contractual requirements governing access and handling of Veteran data. The DOCMP Project Team is required to ensure that all contractors interfacing with DOCMP data are adhering to VA policies and OMB Memorandum M-06-15 and OMB Memorandum M-06-16.

The VA COR has weekly meetings for the review of the contract details and the DOCMP contract is reviewed at least on an annual basis.

Kessler Creative Contract: Contractors receive print files containing PII/PHI for the purpose of printing denial letters. Kessler Creative is responsible for establishing and maintaining NDAs. This information is covered in the MOU/ISA. Per the Kessler Creative contract, the minimum requirements for employees to work in support of this interconnection, to include background investigations and security clearances, will be determined by the contract(s) or requirements governing the support services provided by the vendor. Kessler Creative will be responsible for ensuring that their employees meet the standards set forth in all applicable contracts or requirements and for continuously monitoring and tracking the status of all Kessler Creative employees relevant to this interconnection.

CIPM: Contractors scan documents. Contractors sign NDAs during the onboarding.

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.

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

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 1/22/24
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 10/13/23
5. *The Authorization Termination Date:* 10/12/25
6. *The Risk Review Completion Date:* 10/12/23
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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

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

Not Applicable

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

DOCMP uses cloud technology. The cloud model is Infrastructure as a Service(IaaS) through VA Enterprise Cloud (VAEC) AWS Government. VAEC AWS government is FedRAMP approved.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). ***(Refer to question 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

The Hosting Cloud Service Provider is VA Enterprise Cloud (VAEC) AWS Government.

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.

Yes. All data related to VA government cloud accounts is owned by the government.

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.

This is not applicable as DOCMP is not a cloud provider.

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).

DOCMP does not use RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

ELLER PAMINTUAN

Digitally signed by ELLER PAMINTUAN
Date: 2025.04.15 09:27:32 -06'00'

Privacy Officer, Eller Pamintuan

AMINE MESSAOUDI

Digitally signed by AMINE MESSAOUDI
Date: 2025.04.15 10:43:36 -05'00'

Information System Security Officer, Amine Messaoudi

JEFFREY RABINOWITZ

Digitally signed by JEFFREY RABINOWITZ
Date: 2025.04.15 12:29:55 -04'00'

Information System Owner, Jeffrey Rabinowitz

APPENDIX A-6.1

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

Notice of Privacy Practices are provided at the point of service.

- VHA Privacy Notice: https://department.va.gov/privacy/va-privacy-policies/
- VA Privacy Impact Assessment: https://www.oprm.va.gov/privacy/pia.aspx
- VHA Systems of Records Notice: https://department.va.gov/privacy/system-of-records-notices/

SORNS

https://department.va.gov/privacy/system-of-records-notices/

23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015); https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf
24VA10A7, Patient Medical Records - VA (10-2-2020); https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015); https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020); https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13/2018); https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf
147VA10, Enrollment and Eligibility Records - VA (8-17-2021); https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)