Privacy Impact Assessment for the VA IT System called:

Delivery Operations Claims Management Platform (DOCMP)

Veterans Health Administration

Office of Integrated Veteran Care (IVC)

Date PIA submitted for review:

February 21, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michael Hartmann	Michael.hartmann@va.gov	(303)780-4753
Information System Security Officer (ISSO)	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?" and will be published online to accompany the PIA link.

The Delivery Operations Claims Management Platform 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 the adjudication of claims by allowing business rules to be implemented which assists with quicker processing. In addition to the business rule process these components allows for reports to be created which assists several teams in pulling necessary information as it relates to all aspects of claims including cost, eligibility, and payment data.

Overview

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

1 General Description

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

Delivery Operations Claims Management Platform (DOCMP) system is part of the Office of Integrated Veteran Care (IVC)/Office of Information and Technology (OI&T), Veterans Health Administration.

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

DOCMP will host multiple projects for the VA starting with what was formally known as Document and Process Enabled Repositories (DAPER). DOCMP supports the business function of providing Consolidated Mail Outpatient Pharmacy Services and Pharmacy Benefits Management Systems Oversight.

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

VA owned and VA Operated

2. Information Collection and Sharing

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

3.6 million Veterans and Family Members

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

The Delivery Operations Claims Management Platform is a suite of claims processing components and related applications within the Office of Integrated Veteran Care (IVC) supporting Claims Processing System. This platform assists with the adjudication of claims by allowing business rules to be implemented which assists with quicker processing. In addition to the business rule process these components allows for reports to be created which assists several teams in pulling necessary information as it relates to all aspects of claims including cost, eligibility, and payment data.

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

Information is stored and can be accessed by interconnected Veteran Health Systems as required to provide care.

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

The system is operated through VAEC AWS.

3. Legal Authority and SORN

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

The purpose of the system is consistent with the financial management provisions of title 31, United States Code, chapter 37, 31 U.S.C.3102, 31 U.S.C. 3101 the pay administration provisions of title 5, United States Code, chapter 55; U.S.C 301, Title 26 U.S.C 61. Special provisions relating to VA benefits in Title 38, United States Code, chapter 53, Sections and 31, 109, 111, 304, 501, 501(a), 501(b), 1151 1703, 1705, 1710, 1712, 1717, 1720, 1720G, 1721, 1722, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 1802, 1803, 1812, 1813, 1821, 3102, 5317, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7301(a) 7332, and 8131–8137. 38 Public Law 103–446 section 107 and Public Law 111–163 section 101. 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.

23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015) - 24VA10A7, Patient Medical Records - VA (10-2-2020) 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015) - 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020) - 88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13/2018) - 147VA10, Enrollment and Eligibility Records - VA (8-17-2021)

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

No modifications are needed for the SORNs and cloud technologies are covered for cloud usage.

D. System Changes

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

The PIA is a result of new system creation

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

No. The PIA is a result of new system creation

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information Account Numbers
- Admission/Discharge Date
- Diagnosis/Billing Code
- Common Procedure Code
- Diagnosis code
- Healthcare Provider Name
- Outpatient Encounter Date
- Prescription Data
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☒ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☐ Race/Ethnicity
- ☒ Tax Identification Number
- ☒ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

PII Mapping of Components (Servers/Database)

Delivery Operations Claims Management Platform consists of **9** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Delivery Operations Claims Management Platform** and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
RightFax	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Personal Phone Number(s), Personal Fax Number, Personal Email address	Eligibility and medication disbursement of medication	System is internal to VA. Only approved employees and contractors have access to the system.
Meds by Mail (MbM) Clients	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Personal Phone Number(s), Personal Fax Number, Personal Email address, Medical Record Numbers, Health Insurance beneficiary numbers, Account Numbers, Certificate/License Numbers	Eligibility and medication disbursement of medication	System is internal to VA. Only approved employees and contractors have access to the system.

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Office of Integrated Veteran Care (IVC)	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Personal Phone number(s), Personal Fax number, Personal Email address, Health Insurance Beneficiary Numbers, Account Numbers, Certificate/License Numbers, Medical Records, Medical Record Number.	Eligibility and Medication disbursement of medication	System is internal to VA. Only approved employees and contractors have access to the system.
Fiscal clients	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Diagnosis code, Common Procedure Code, Health Insurance Beneficiary Numbers, Personal Mailing Address, Admission/Discharge Date, Outpatient Encounter Date, Healthcare Provider Name, Tax Identification Number	Eligibility and Medication disbursement of medication	System is internal to VA. Only approved employees and contractors have access to the system.

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
DeepSee clients	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Personal Phone Number, Personal Fax Number, Personal Email Address, Health Insurance Beneficiary Numbers, Account Numbers, Certificate/License numbers, Medications, Medical Records, Medical Record Number	Eligibility and Medication disbursement of medication	System is internal to VA. Only approved employees and contractors have access to the system.
Front End Capture	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Personal Phone Number(s), Personal Fax Number, Personal Email Address, Health Insurance Beneficiary Numbers, Account Numbers, Certificate/License Numbers, Medical Records, Medical Record Number	Eligibility and Medication disbursement of medication	System is internal to VA. Only approved employees and contractors have access to the system.

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
HACR1PSVR – 1 of 2 - Claims Processing & Eligibility (CP&E)	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Health Insurance Beneficiary Numbers, Coded Billing Information, Prescription data.	Eligibility and Medication disbursement of medication	System is internal to VA. Only approved employees and contractors have access to the system.
HACR1PSVR – 2 of 2 - Claims Processing & Eligibility (CP&E)	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Personal Phone Number(s), Personal Fax Number, Personal Email address	Eligibility and Medication disbursement of medication	System is internal to the VA. Only approved employees and contractors have access to the system.
Opex Scanners (WY & GA)	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Health Insurance Beneficiary Numbers, Coded Financial Information, Prescription Data	Eligibility and Medication disbursement of medication	System is internal to the VA. Only approved employees and contractors have access to the system.

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

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

The data is obtained by the individual Beneficiary via VA Form 10-0426 sent in various ways. Forms can be sent via U.S. Mail. Healthcare providers send in prescriptions via electronic prescribing (e-Rx) contract or direct faxing to the IVC RightFax account. RightFax takes the sent fax and packages it and sends it to the DOCMP system. DOCMP initiates a query to IVC Veterans Information Systems and Technology Architecture (VistA) to verify Beneficiary data that already exists. IVC VistA verifies the patient data and sends it back to DOCMP. The staff at the processing centers log in to a VA internal web portal that cannot be accessed outside the VA network. Staff can view and route the prescriptions through a designed workflow.

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.

DOCMP does not use a commercial aggregator of information or external source. Data is taken from VistA.

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

The System does not generate scores, analysis, or aggregate reporting.

1.3 How is the information collected?

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

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

Information is collected from providers and individuals. Information is submitted via electronic submission through RightFax.VA Form 10-0426 is provided via U.S. Mail from the Beneficiary or faxed from healthcare provider offices. Beneficiary data already exists in IVC VistA. The beneficiary completes the form to participate in the MbM program.

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

VA Form 10-0426 currently does not have an OMB control number, a Privacy Act statement, nor a Paperwork Reduction Act statement.

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

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

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

Information is checked using a combination of automated and manual checks. The form and or prescription images in DOCMP are checked against existing data in IVC VistA. If they do not match the prescription will not be filled. VA Form 10-0426 if incorrectly completed is flagged by an automated system. Data Field Identifiers are received by DOCMP from the VistA system. The incorrect form is then manually reviewed. Contact would be made with VistA owner to correct data.

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

DOCMP does not receive or share data with any external organization.

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

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Incorrect patient or medical information in the VA Form 10-0426.

Mitigation: VA Form 10-0426 if incorrectly completed is flagged by an automated system. Data Field Identifiers are received by DOCMP from the VistA system. The incorrect form is then manually reviewed. Contact would be made with VistA owner to correct data.

Section 2. Uses of the Information

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

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

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

The data listed in section 1.1 is re-listed below with an explanation of how each piece of information is used to process prescriptions sent to DOCMP. There are no external interfaces with DOCMP.

Name: Used for Beneficiary identification (internal use only);
Social Security Number: Used to verify Beneficiary identity and as a file number for the Beneficiary (internal use only);
Date of Birth: Used for Beneficiary identification (internal use only);
Personal Mailing Address: Used to verify the correct address to mail the prescription;
Personal Phone Number(s): Used to give the pharmacist an easy way to contact the Beneficiary if necessary to clarify pharmacy issues;
Personal Fax Number: Forms are received by fax number. It is inherent.;

Medications: Used as a drug interactions pharmacy reference and.to cross reference the patients' medical conditions with the pharmacological potential drug side effects;
Previous Medical Records: Used to cross reference the patients' medical conditions with the pharmacological potential drug side effects.;
potential drug side effects;
Personal Email Address: to properly identify, adjudicated and pay claims;
Beneficiary: Used for Beneficiary identification;
Account number: Used for identification;
Certificate: Legal binding document identification ;
Certificate/License: Used for external provided credentialing;
Admit/Discharge Date: Identify health care information status;
Outpatient Date: to provide actual dates for adjudication and pay claims;
Healthcare Provider Name: to properly identify, adjudicated and pay claims;
Healthcare Provider Tax ID: to properly identify, adjudicated and pay claims;
Diagnosis/Billing Code: to properly identify, adjudicated and pay claims;
Common Procedure Code: to properly identify, adjudicated and pay claims

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

DeepSee (Cache and Ensemble) is used to embed business intelligence (BI) into DOCMP so that users can ask and answer sophisticated questions of their data. DeepSee utilizes several layers of dashboards and analytic tools to provide DOCMP administrators the ability to monitor and track workflow tasks. Updated medical information is available to "need to know" government employees such as the ones that work in the MbM distribution centers processing the prescriptions.

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 is the information in the system secured?

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

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

DOCMP limits traffic to internal users. Access to PII is provided to those staff that is 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?

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?

DOCMP limits access to PII to only those staff that is deemed necessary for MbM processing centers and VAEC AWS to do their jobs as determined by their management team and job description. Supervisors request access for staff by role.

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

System documentation includes detailed system design and the user guides that specify those areas of the system that contain PII and PHI, as well as how it is used by the MbM staff. Additionally, user roles are implemented to restrict user's access to only specific information required to perform their job function.

2.4c Does access require manager approval?

Yes, this elevated privilege group is granted permission through the Electronic Permission Access System (EPAS) upon supervisor's approval.

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

Addition, modification, or removal from Access is completed upon receipt of an updated MyVAElevatedPrivilege ePAS ticket that modifies authorization. MyVAElevatedPrivilege ePAS authorization is used as a queue for DOCMP admin(s) to modify user memberships. 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. DOCMP administrators receive ePAS approved changes for removal from Access.

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

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*

There are no external interfaces with DOCMP. Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Fax Number, Personal Email Address, Beneficiary Health Insurance Beneficiary Numbers, Account numbers, Provider Certificate/License numbers, Medications, Medical Records, Admit/Discharge, Outpatient Date, Healthcare Provider Name, Healthcare Provider Tax ID, Diagnosis/Billing Code, Common Procedure Code. Sponsor information is sometimes submitted as an element, this information is not required, and so it is purged but could be maintained. It is a small percentage. This information is not required.

3.2 How long is information retained?

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

Meds by Mail: Claim Fil-Records1260 Civilian Health and Medical Care Program; 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) Medical File6000 Health Information Management (HIM) Service, 6000.1. Health Records Folder File or CHR (Consolidated Health Record). This records series contain all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. a. Health Records Folder. Temporary; retain in VA health care facility until 3 years after last episode of care, and then convert to an inactive medical record. (N1-15-91-6, Item 1a) d. Inactive Health Record. Temporary; retire annually to the records storage facility. If not recalled by the

accessioning facility for reactivation, destroy by WITNESS DISPOSAL72 years after retirement (75 after the last episode of care). (N1-15-91-6, Item 1d)6000.2. Electronic Health Record (EHR). a. Input. (1) Paper Source Documents. (a) Hardcopy version of information manually inputted into the Electronic Health Record System (EHRS). Temporary; destroy after verification of accurate entry of information into EHRS. (N1-15-02-3, Item 1a) (b) Hardcopy version of information scanned onto optical disk or other magnetic media. Temporary; destroy after verification of accurate scan onto optical disk or other magnetic media. (N1-15-02-3, Item 1b) Pharmacy Record File:7400.11. Prescription File. Temporary; destroy after 3 years. (NN-166-175)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 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

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

Yes

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

Meds by Mail. This system retains records per the VA Records Control Schedule 10-1 section 7400.11. Prescription File: Temporary; destroy after 3 years. (NN-166-175) DAPERVHA Record Control Schedule (RCS) 10–1 https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf; 1260.1 Civilian Health and Medical Care Program. Electronic Records. (Master Files) Electronic records produced from scanned documents or records received electronically (optical disk, magnetic tape, or other electronic medium). Temporary; destroy 6 years after all individuals in the record become ineligible for program benefits.

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.

Meds by Mail Paper records are maintained for 4 months after scanning and verification is complete and then is destroyed by an approved shredding vendor. Controlled prescriptions are held a period of 3 years. DOCMP images will be purged after 6 years after all individuals in the record become ineligible for program benefits. Paper records are destroyed after successfully scanned to electronic medium. 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 VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA 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. Digital media is shredded or sent out for destruction. Electronic records are retained permanently. https://www.va.gov/vapubs/search_action.cfm?dType=1

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 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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

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

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

<u>Principle of Minimization:</u> Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

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

Follow the format below:

Privacy Risk: If data is maintained within the DOCMP system for a longer time-period than what is needed or required, then the risk that the information will be compromised, breached, or unintentionally released to unauthorized individuals increases.

Mitigation: DOCMP system adheres to information security requirements instituted by the VA OI&T to secure data with PII in a FISMA-Moderate environment. Because the data is retained indefinitely, a Backup Plan and Restore Plan are in place. At a minimum, the plan includes the requirement to save data for the backup and recovery of information stored on the IVC VistA 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).

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Benefits Administration RightFax	Eligibility and medication disbursement of medication	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Personal Phone Number(s), Personal Fax Numbers, Personal Email address.	VA Network, Common Internet File System (CIFS); Fax and ePrescribing
Veterans Health Administration Meds by Mail (MbM) clients	Eligibility and medication disbursement of medication	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Addresses, Personal Phone Number(s), Personal Fax Numbers, Personal Email address, Medical records, Health Insurance beneficiary numbers, Account Numbers, Certificate/License Numbers.	VA Network, Hypertext Transfer Protocol Secure (HTTPS)
Veterans Health Administration IVC	Eligibility and medication disbursement of medication	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Personal Phone number(s), Personal Fax numbers, Personal Email address, Health Insurance Beneficiary Numbers, Account Numbers, Certificate/License Numbers, Medical Records.	VA Network, Hypertext Transfer Protocol Secure (HTTPS)

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration Fiscal clients	Eligibility and medication disbursement of medication	Name, Social Security Number (SSN), Date of Birth (DOB), Diagnosis code, Common Procedure Code, Health Insurance Beneficiary Numbers, Mailing Addresses, Address, Admission/Discharge Date, Outpatient Encounter Date, Healthcare Provider Name, Tax Identification.	VA Network, Hypertext Transfer Protocol Secure (HTTPS)
Veterans Health Administration DeepSee clients	Eligibility and medication disbursement of medication	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Personal Phone Number(s), Personal Fax Number, Personal Email Address, Health Insurance Beneficiary Number, Account Numbers, Certificate/License Numbers, Medications, Medical Records	VA Network, Hypertext Transfer Protocol Secure (HTTPS)
Veterans Health Administration Front End Capture	Eligibility and medication disbursement of medication	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Personal Phone Number(s), Personal Fax Number, Personal Email Address, Health Insurance Beneficiary Number, Account Numbers, Certificate/License Numbers, Medical Records.	VA Network, Common Internet File System (CIFS)
Veterans Health Administration Processing & Eligibility (CP&E) 1 of 2	Eligibility and medication disbursement of medication	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Health Insurance Beneficiary Numbers, Coded Billing Information, Prescription data.	VA Network, Cache, Enterprise Cache Protocol (ECP) Hypertext Transfer Protocol Secure (HTTPS)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Veterans Health Administration Processing & Eligibility (CP&E) 2 of 2	Eligibility and medication disbursement of medication	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Mailing Address, Health Insurance Beneficiary Numbers, Coded Billing Information, Prescription data.	VA Network, Cache, Enterprise Cache Protocol (ECP) Hypertext Transfer Protocol Secure (HTTPS)
Veterans Health Administration Opex Scanners (WY & GA)	Eligibility and medication disbursement of medication	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Health Insurance Beneficiary Numbers, Coded Billing Information, Prescription Data.	VA Network, Common Internet File System (CIFS); Prescription Scanned documents

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Privacy information may be inadvertently released to unauthorized individuals.

Mitigation: The DOCMP system ensures strict access to information by enforcing thorough access control and requirements for end users. DOCMP limits traffic to internal users. Access to PII is provided to those staff that is deemed necessary via ePAS. The VA limits access of PII only to staff as appropriate to their role in Veteran Care.

Individual administrator user IDs and access are provided only based on need.

DOCMP has built-in controls to limit 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 Privacy, HIPAA, and information security 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 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

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

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

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

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

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

Data Shared with External Organizations

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

	program office or IT system		***external sharing (can be more than one)***	
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 6. Notice

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

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

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

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the

Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

This Privacy Impact Assessment (PIA) 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."

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

- VHA Privacy Notice: https://www.oprm.va.gov/privacy/about_privacy.aspx
- VA Privacy Impact Assessment: https://www.oprm.va.gov/privacy/pia.aspx
- VHA Systems of Records Notice: https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf

SORNS

23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015) 24VA10A7, Patient Medical Records - VA (10-2-2020) 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015) 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12-23-2020) 88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8-13/2018) 147VA10, Enrollment and Eligibility Records - VA (8-17-2021)

The VHA IVC CHAMPVA Guide:
https://www.va.gov/COMMUNITYCARE/docs/pubfiles/programguides/champva_guide.pdf

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

Notice is provided at point of service.

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

Notice is provided at the point of service. The DOCMP System interfaces with other systems and does not provide notice to individuals.

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 Directive1605.01 'Privacy and Release Information' lists the rights of beneficiaries to request the VHA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. Beneficiaries have the right to refuse to disclose their SSNs to the VHA. The individual shall not be 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)). Additionally, a link to the VA Notice of Privacy Practices is provided at Appendix A

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

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

VHA Directive 1605.01, Privacy and Release Information list the rights of Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. Beneficiaries have the right to refuse to disclose their SSNs to the VHA. The individual shall not be 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)). CHAMPVA Guide: Your Privacy Rights. Review your health information. Obtain a copy of your health information. Request that your health information be amended or corrected. Request that we not use or disclose your health information. Request that we provide your health information to you in an alternative way or at an alternative location in a confidential manner. An accounting or list of disclosures of your health information. Receive our VA Notice of Privacy Practices upon request. Additionally, a link to the VA Notice of Privacy Practices is provided at Appendix A.

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

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

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: Sufficient notice of incident is not provided to the patient. Incidents occur when collected information is used for an unauthorized purpose.

Mitigation: The VA Form 10-0426 is submitted to correct the privacy statement and to receive OMB approval. All Personnel are trained annually, and incidents are reported to the Privacy Office for investigation.

Section 7. Access, Redress, and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?
These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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

VHA Directive 1605.01: Privacy and Release Information states the rights of Beneficiaries to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review or seek copies of records must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access to data must be delivered to, and reviewed by, the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must include the signature of the requester, date of birth, copy of signed government identification, state what is request and the period of the information requested. Mail requests for eligibility information/records to: CHAMPVA Eligibility PO Box 469028 Denver, CO 80246-9028. Mail requests for CHAMPVA billing/claim records to: VHA Office of Integrated Veteran Care Privacy/FOIA Office, PO Box 469060 Denver, CO 80246-9060. Requests for medical and pharmacy records contact your servicing medical provider. For Veteran billing records contact the VA Financial Services Center (FSC) Privacy Office by via email at vafscprivacyofficer@va.gov for secure submission methods. 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 authoritative source for the data is IVC VistA. If data stored in the authoritative sources are erroneous, the MbM personnel can take a note, but cannot correct inaccurate or erroneous information stored in IVC VistA. However, if a correction is requested by a Beneficiary or Provider, then such a request must be in writing and it must adequately describe the specific information that the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.VHA Directive 1605.01, Appendix D: Privacy and Release Information, Section 5 lists the rights of Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. The CHAMPVA Guide provides: Mail Requests for information/document to: Eligibility: CHAMPVA Eligibility PO Box 469028 Denver, CO 80246-9028 Billing/Claim Records: VHA Office of Community Care privacy Office (Attn: Privacy) PO Box 469060 Denver, CO 80246-9060 Medical/Pharmacy Records: Requests for medical and pharmacy records contact your servicing medical provider. Mail all request for billing records (to include claims processing records) to the VHA Office of Community Care privacy Office, (Attn: Privacy) PO Box 469060, Denver, CO 80246 Requests for medical and pharmacy records contact your servicing medical provider.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that

even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The authoritative source for the data is IVC VistA. If data stored in the authoritative sources are erroneous, the MbM personnel can take a note, but cannot correct inaccurate or erroneous information stored in IVC VistA. However, if a correction is requested by a beneficiary or provider, then such a request must be in writing and it must adequately describe the specific information that the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, and needs to be date stamped and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. CHAMPVA Guide provides: Mail Requests for information/document to: Eligibility: CHAMPVA Eligibility PO Box 469028 Denver, CO 80246-9028 Billing/Claim Records: VHA Office of Community Care privacy Office (Attn: Privacy) PO Box 469060 Denver, CO 80246-9060 Medical/Pharmacy Records: Requests for medical and pharmacy records contact your servicing medical provider. Mail all request for billing records (to include claims processing records) to the VHA Office of Community Care privacy Office, (Attn: Privacy) PO Box 469060, Denver, CO 80246 Requests for medical and pharmacy records contact your servicing medical provider. Additionally, a link to the VA Notice of Privacy Practices is provided at Appendix A.

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

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

If the beneficiary discovers that incorrect information was provided during intake, they simply follow the same contact procedures in section 7.3 (also re-stated below), and state that the documentation they are now providing supersedes those previously provided. If a Beneficiary discovers that incorrect information was provided during the intake process, the request must be in writing and adequately describe the specific information the Beneficiary believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and 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. CHAMPVA Guide provides: Mail Requests for information/document to: Eligibility: CHAMPVA Eligibility PO Box 469028 Denver, CO 80246-9028 Billing/Claim Records: VHA Office of Community Care privacy Office (Attn: Privacy) PO Box 469060 Denver, CO 80246-9060

Medical/Pharmacy Records: Requests for medical and pharmacy records contact your servicing medical provider. Mail all request for billing records (to include claims processing records) to the VHA Office of Community Care privacy Office, (Attn: Privacy) PO Box 469060, Denver, CO 80246 Requests for medical and pharmacy records contact your servicing medical provider.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that incorrect information might be accidentally recorded in a beneficiary's record.

Mitigation: A beneficiary who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or who wants to review the contents of such a record, should submit a written request or apply in person to the VA health care facility (or directly to the VHA) where care was rendered. The request should include the patient's full name, SSN, and return address. The request will be reviewed and processed.

Section 8. Technical Access and Security

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

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

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

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

User access is provided by the DOCMP System Administrators following receipt of request from individuals with supervisor concurrence. The DOCMP system implements auditing which tracks user access to the system and all data accessed. The information is mapped in the audit record. Clearance procedures are implemented to monitor access, and accounts are disabled after 30 days of inactivity.

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

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

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

VA contracted pharmacy personnel have no access to development. Contractors do have access to the live production system to perform prescription activities. The following steps are required before contractors can gain access to the system: Contractors must take and pass training on privacy, HIPAA, information security, and government ethics and role-based training based on support role to the system. Contractors must have signed the Non-Disclosure Agreement (NDA) and VA Information Security Rules of Behavior (RoB). Contractors must have successfully completed VA contractor background security investigation as per the Position Designation Automated Tool (PDT). Once complete, a request is submitted for access before access is granted to the DOCMP system. VA owns the data. The DOCMP system extracts VA data from VA source applications and then secures that data within the DOCMP system. The VA COR has weekly meetings for the review of the contract details and this contract is reviewed at least on an annual basis. There shall be a regular review of user access to evaluate whether users are active in the environment. If a user is not active, the account will be terminated. A designated VA Project point of contact (POC) is the only person who may submit account creation requests for accountability purposes. Contractor access to the system expires at the end of the contract duration or earlier.

Applicable procedures from VA Handbook 6500.6 on contractor security requirements: Information generated by a contractor or subcontractor as part of the contractor/subcontractor's normal business operations, such as health record information created in the course of providing treatment or health care services to VA's Veterans is subject to review to determine if the information is owned by VA and subject to VA security policy. VA sensitive information that has been properly disclosed by VA to the contractor is not subject to the VAAR security clause. If the information is not owned by VA, the requirements outlined in this Handbook do not apply and the VAAR security clause should not be added to the contract. The CO, the PO, and if required, Regional Counsel can be consulted. VA OIG counsel will conduct the review for the OIG generated contracts.

B.) VA requires that facilities and program offices ensure that contractors, subcontractors, and third-party servicers or associates, or on behalf of any of these entities, regardless of format or whether the VA information resides on a VA system or contractor/subcontractor's electronic information system(s) operating for or on VA's behalf, employ adequate security controls as appropriate in accordance with VA directives and handbooks, regulations, guidance, and established service level agreements.

C.). Information security requirements must be considered in all phases or stages of VA's procurement process. The applicable Program Manager, Information System Owner, and Information Owner are responsible for ensuring that the solicitation document includes the appropriate information security and privacy requirements. The information security requirements must be sufficiently detailed to enable service providers to understand what is required. A general statement that the service provider must agree to comply with applicable requirements is not acceptable. See Appendix C for a catalog of security and privacy language statements that have been developed, reviewed, and approved and can be used in contracts, as appropriate. This language summarizes for the contractors the most important Federal and VA policy issues that need to be addressed, as appropriate, in contracts to ensure adequate security and privacy controls are included in the contract vehicle. Additional security or privacy language can be added, as required. Program managers, project designers, and acquisition professionals must take security requirements, measures, and controls into account when designing and making agency acquisitions; appropriate security controls drive requirements, specifications, deliverables, and costs. Acquisition staffs need to consult information security officials to determine what level of security and which security controls may be required in this process. VA Handbook 6500, Information Security Program, provides the security requirements and policy for VA.

D.) The applicable VA Program Manager, Information System Owner, Information Owner, the CO, PO, ISO, and the Contracting Officer's Technical Representative (COTR) are responsible for ensuring that VA information system security and privacy requirements, as appropriate, are implemented and complied with per the requirements detailed in the contract. Compliance and Records Management Officers should also be contacted, as appropriate, to ensure the requirements and language they require are included in the contract.

E.) VA requires that all facilities and program offices monitor information security control compliance of their respective contracts and acquisitions by doing the following:

(1) Adhere to the security and privacy contract language as outlined in the contracts.

(2) Ensure that COs work with their COTR, ISO, and PO and other applicable staff to complete Appendix A for all service acquisitions and contracts. This appendix assists in determining the security requirements for VA acquisitions and contracts during the planning phase of the acquisition process. The checklist must be included as part of the overall contract file by the CO for new service acquisitions and contracts and a copy must be maintained in the applicable contracts file and accessible to the COTR, ISO, and PO.

(3) Ensure that contracting officials include VA's approved security clause, Appendix B, into any applicable contracts, if required as indicated by completing Appendix A. NOTE: The security clause in Appendix B is currently undergoing official VA rulemaking by the Office of Acquisitions and Logistics (OA&L). The final version of the clause may be revised after it is presented to the public for review via the Federal Register.

(4) Ensure that contractors, third party partners, and servicers implement the VA security and privacy requirements, as defined in the contract. These requirements can also be added to the contract Statement of Work (SOW). The requirements apply to applicable contracts in which VA sensitive information is stored, generated, transmitted, or exchanged by VA, a contractor, subcontractor or a third-party, or on behalf of any of these entities regardless of format or whether it resides on a VA system or contractor or subcontractor's electronic information system(s) operating for or on the VA's behalf.

(5) Ensure that contractor systems that have negotiated with VA to store, generate, transmit, or exchange VA sensitive information in a contractor developed and maintained system are certified and accredited (authorized), and registered and monitored in VA's Security Management and Reporting Tool (SMART) database that monitors FISMA compliance. The Program Manager and/or the ISO are responsible for contacting the Information Protection and Risk Management's (IPRM) Certification Program Office (CPO) within OI&T to register the system or to answer questions regarding the authorization of systems

(6) Ensure that Certification and Accreditation (Authorization) (C&A), is accomplished in compliance with VA policy (per the results of the completed checklist provided in Appendix A) and VA Handbook 6500.3, Certification and Accreditation of VA Information Systems. The OI&T CPO within the Office of Cyber Security (OCS) must be contacted regarding procedures for C&A (Authorization) of contractor managed systems.

(7) Ensure that the Program Manager, the COTR and the CO, with the assistance of the ISO, monitor compliance with the contract or agreement security requirements throughout the life of the contract. For IT systems, this includes ensuring that annual self-assessments are conducted by the contractor with appropriate Plan of Actions and Milestones (POA&M) initiated and completed.

(8) Ensure that service providers and contractors who have negotiated agreements with VA that involve VA sensitive information, but do not maintain systems that require C&A, complete a Contractor Security Control Assessment (CSCA) within 30 days of contract approval and annually on the due date of the contract renewal. The ISO/COTR or CO can also request that a CSCA be completed by the contractor anytime there are potential security issues identified or suspected by VA or to ensure that applicable security controls are being implemented. The

completion of the CSCA by the contractor is the responsibility of the COTR. The CSCA template is maintained on the IPRM portal under the C&A Section. The COTR can contact the ISO to obtain a copy of the CSCA from the portal or to seek assistance in the completion of the assessment. The completed CSCA must be provided and reviewed by the ISO and by the CPO to ensure that adequate security is being addressed by contractors in situations where the C&A of a system is not applicable. A copy of the CSCA is uploaded by the ISO and maintained in the document section of the SMART database.

(9) Ensure that contractors and third-party servicers accessing VA information sign the Contractor Rules of Behavior, Appendix D. The VA National Rules of Behavior do not need to be signed if the VA Contractor Rules of Behavior" are signed.

(10) Ensure that contractors and third-party service positions receive the proper risk level designation based upon the review of the Position Designation System and Automated Tool (PDAT) established by the Operations, Security, and Preparedness Office (007). Background investigations of all contractors must adhere to the results of the PDAT per VA Directive and Handbook 0710, Personnel Suitability and Security Program.

(11) Ensure that contractors take the required security and privacy training as outlined in Appendix C.

(12) Ensure that all IT procurements, including contracts, are submitted through the IT Acquisition Request System (ITARS), VA's acquisition approval system for review and approval as required by the VA CIO.

(13) Ensure that language is included in appropriate contracts to ensure new acquisitions include Federal Desktop Core Configuration (FDCC) settings and products of information technology providers operate effectively using them.

Link to VA Handbook 6500.6:
http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=471&FType=2

Contractors must take approved VA security training and sign the VA Rules of Behavior document Located in VA Handbook 6500.6 Appendix C.

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 Has Authorization and Accreditation (A&A) been completed for the system? No

8.4a If Yes, provide:

1. *The Security Plan Status:* Please provide response here
2. *The System Security Plan Status Date:* Please provide response here
3. *The Authorization Status:* unauthorized
4. *The Authorization Date:* n/a
5. *The Authorization Termination Date:* n/a
6. *The Risk Review Completion Date:* Please provide response here
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Please provide response here

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.***

Authorization and Accreditation (A&A) is in progress for DOCMP. DAPER has an Authority to Operate until November 28, 2023.

Section 9 – Technology Usage

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

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

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

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)*

A private IaaS through VAEC AWS.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A

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

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

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

N/A

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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

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

No RPA being used.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Michael D Hartmann 1612370

Digitally signed by Michael D Hartmann 1612370
Date: 2023.02.21 15:07:47 -07'00'

Privacy Officer, Michael Hartmann

Amine Messaoudi 1136390

Digitally signed by Amine Messaoudi 1136390
Date: 2023.02.23 09:21:28 -06'00'

Information Systems Security Officer, Amine Messaoudi

JEFFREY RABINOWITZ

Digitally signed by JEFFREY RABINOWITZ
Date: 2023.02.24 09:55:04 -05'00'

Information Systems 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).

- Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES
- 23VA10NB3, Non–VA Care (Fee) Records – VA (7/30/2015)
- 24VA10A7, Patient Medical Records – VA (10/2/2020)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
- 88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
- 147VA10, Enrollment and Eligibility Records - VA (8/17/2021)

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices