



Privacy Impact Assessment for the VA IT System called:

OM FSC DMS Assessing  
VA Central Office (VACO)  
Financial Technology Service  
eMASS ID # 160

Date PIA submitted for review:

January 07, 2025

System Contacts:

*System Contacts*

	Name	E-mail	Phone Number
Privacy Officer	Morla Roberts	morla.roberts@va.gov	512-554-8583
Information System Security Officer (ISSO)	Ronald Murray	Ronald.Murray2@va.gov	512-460-5081
Information System Owner	Jonathan M. Lindow	Jonathan.Lindow@va.gov	512-568-0626

## Abstract

*The abstract provides the simplest explanation for “what does the system do for VA?”.*

OM FSC Document Management System (DMS) Assessing process documents from various customers that are scanned, faxed, emailed, and imported. Application is used to index and archive documents. It's comprised of two front-end tools (.Net and Pega) which, use FileNet as their content repository to store data. The system intakes scanned and faxed documents from various customers.

## Overview

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

### 1 General Description

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

Document Management System known as DMS is used to process documents that are scanned, faxed, emailed, and imported as examples listed in 1.2b. DMS is an enterprise-wide application used by business users within VA FSC and FTS provides directions.

The scanned or faxed documents are listed in 3.2 and used to process a request.

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

Financial Technology Service. In addition, this project is VA Owned and VA Operated.

### 2. Information Collection and Sharing

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

<b>DMS Workflow</b>	<b>expected number of individuals whose information is stored in the system</b>	<b>a brief description of the typical client or affected individual</b>	<b>A general description of the information in the IT system</b>	<b>the purpose for collecting this information</b>
Vendor	467216	Individual, care givers, VA employees and Veterans who want to be part of Vendor File for receiving payments	VENDOR ID	To register in Vendor File for individuals to receive payments

<i>Recertification</i>	<i>Approximately 6500</i>	<i>Individuals, Veterans and Vendors</i>	<i>VENDOR ID</i>	<i>To identify the entities who potentially did not receive a paper check</i>
<i>OGA</i>	<i>1021365</i>	<i>Detainees</i>	<i>Alien ID, First Name, Last Name, TIN</i>	<i>To process detainees' medical claims</i>
<i>Camp Lejeune</i>	<i>91157</i>	<i>Camp Lejeune family member</i>	<i>Member ID, Member First Name, Member Last Name</i>	<i>To process Family member medical claims</i>
<i>Accounting</i>	<i>4594</i>	<i>VA Employees</i>	<i>Employee Name</i>	<i>To identify the individual designated as an agent cashier or director at the station.</i>
<i>Retirement Suite</i>	<i>484923</i>	<i>Nationwide VA employees</i>	<i>SSN, Name, DOB, Station, Email Address</i>	<i>Accurate computation of retirement benefits</i>
<i>CPAC</i>	<i>484923</i>	<i>CPAC</i>	<i>VENDOR ID, VENDOR_NAME</i>	<i>To process veterans, hospital claims</i>

<b>Check if Applicable</b>	<b>Demographic of individuals</b>
<input checked="" type="checkbox"/>	Veterans or Dependents
<input checked="" type="checkbox"/>	VA Employees
<input checked="" type="checkbox"/>	Clinical Trainees
<input checked="" type="checkbox"/>	VA Contractors
<input checked="" type="checkbox"/>	Members of the Public/Individuals
<input checked="" type="checkbox"/>	Volunteers

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

See chart in 2C.

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

See chart in 2C.

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

No

G. *Is the system operated in more than one site to include primary and secondary site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?*

System is only at Financial Service Center

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

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 31 U.S. Code 3512- Executive Agency Accounting and other Financial Management Reports and Plans; Federal Managers' Financial Integrity Act section 2 of 1982; Federal Financial Management Improvement Act of 1996; E-Government Act of 2002 title III., Federal Information Security Modernization Act (FISMA) of 2014; Clinger Cohen Act of 1996; 38 CFR part 17 17.120–17.132; OMB Circular A–123, Management's Responsibility for Internal Control.

<https://www.govinfo.gov/content/pkg/FR-2023-08-31/pdf/2023-18807.pdf>

Individuals Submitting Invoices - Vouchers for Payment -VA (13VA047

I. *What is the SORN?*

VA (13VA047

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

No

### 4. *System Changes*

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

Yes

No

if yes, <<ADD ANSWER HERE>>

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

Yes

No

if yes, <<ADD ANSWER HERE>>

## Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (II), 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://vawww.va.gov/vapubs/>). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

- |   |  |  |
|---|--|--|
| <input checked="" type="checkbox"/> Name  | <input checked="" type="checkbox"/> Health Insurance Beneficiary Numbers     | <input type="checkbox"/> Military History/Service Connection   |
| <input checked="" type="checkbox"/> Full Social Security Number   | Account Numbers  | <input type="checkbox"/> Next of Kin   |
| <input type="checkbox"/> Partial Social Security Number   | <input checked="" type="checkbox"/> Certificate/License numbers <sup>1</sup> | <input type="checkbox"/> Date of Death   |
| <input checked="" type="checkbox"/> Date of Birth   | <input type="checkbox"/> Vehicle License Plate Number                        | <input type="checkbox"/> Business Email Address  |
| <input checked="" type="checkbox"/> Mother's Maiden Name  | <input type="checkbox"/> Internet Protocol (IP) Address Numbers              | <input type="checkbox"/> Electronic Data Interchange Personal Identifier (EDIPI) <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Personal Mailing Address  | <input checked="" type="checkbox"/> Medications                              | Other Data Elements (list below)   |
| <input checked="" type="checkbox"/> Personal Phone Number(s)  | <input checked="" type="checkbox"/> Medical Records                          |  |
| <input type="checkbox"/> Personal Fax Number  | <input type="checkbox"/> Race/Ethnicity                                      |  |
| <input type="checkbox"/> Personal Email Address   | <input checked="" type="checkbox"/> Tax Identification Number                |  |
| <input type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a different individual) | <input checked="" type="checkbox"/> Medical Record Number                    |  |
| <input checked="" type="checkbox"/> Financial Information   | <input type="checkbox"/> Gender/Sex  |  |
|   | <input type="checkbox"/> Integrated Control Number (ICN)                     |  |

---

<sup>1</sup> \*Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

Other PII/PHI data elements:

Additional Data elements

- Driver's License
- Place of Birth
- Business Telephone Number
- Business Mailing Address
- Business Email Address
- Geographical Indicators
- Medical Information

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

## 1.2 List the sources of the information in the system

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

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

**Camp Lejeune Family Member (CLFM):** Application submitted by Camp Lejeune Family Member (CLFM), documents submitted by CLFM such as birth certificate, DD 214 Statements of Military service (veteran sponsor), medical records/documents, Treating Physician Report Form submitted by CLFM or physician, medical claims submitted by CLFM or providers, VA employees and the members themselves, VA10091 submitted by CLFM. Data from Medical records and Treating Physician Report Form submitted by Physicians and providers are required to qualify for the CLFM program.

**Other Government Agencies (OGA):** Medical claims submitted by non-VA providers, W-9s (Requests for Taxpayer Identification number) submitted by non-VA providers, SF 3881s (Vendor Miscellaneous Enrollment Form) submitted by non-VA providers—all required for reimbursement for medical services rendered to (Dept of Homeland Security) DHS and (Office of Refugee and Resettlement) ORR detainees.

**Vendorizing:** Directly from- Veterans, VA Employees, VA Contractors, Individuals, Federal and Foreign Vendors.

**DMS Central:** Sources of information include – user input via the webform. The system does not have any database or service calls to determine if the information is valid.

**Recertification:** VA Medical Facilities fax in requests, 1133 claims forms are scanned or faxed in using RightFax. Recertification is used for tracking requests and results of those requests.

**Payroll:** The paper documents come from Stations transitioning to the FSC for Payroll services.

**Travel:** Commercial payment information submitted by the vendor for payment purposes.

**Consolidated Patient Account Center (CPAC):** CPAC stations submit the following documents: Bankruptcy, First Party Refund, Medical EOB, Pharmacy EOB, Probate, Third Party Refund, Write offs, Waivers, No Pay EOBs.

**Retirement Suite:** Information is provided by Station Payroll Departments, Station Human Resources (HR) Departments, Office of Personnel Management, Defense Finance Accounting Service, and VA FSC Payroll Support Operations.

**Audit of the Administrative and Loan Accounting (ALAC):** VBA Regional Offices (ROs) communicate and submit documentation to ALAC for processing out-of-system financial requests. ALAC reviews and processes the requests received and archives the documentation. Access to archived documentation ensures each financial transaction processed for a RO is historically recorded and available for auditability purposes, and research.

**Local Accounting:** To identify the individual designated as an agent cashier or director at the station.

*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.*

- Information is supplied by individual.
- Information may come from HR as new employee on boarding or customer service representative on behalf of individual.
- Family member or medical provider can mail or fax in for reimbursements
- Information may come by mail, fax, & email from Office of Personnel Management to correct an error on previous issued retirement document.
- Information comes from other sources because an individual uses different resources or offices to gain or processes request.
- Regional Offices submit support documentation for accounting transactions processed in FMS in order to meet retention policy and internal audit requirements

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

The system is a source of information gathering.

### **1.3 Methods of information collection**

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

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

Documents are scanned, faxed, and imported into the FileNet repository by Enterprise Service Bus. In addition, the documents are routed, processed, and displayed to the user by DMS.

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

Information is not collected on a form and is not subject to the Paperwork Reduction Act.

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

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

*1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency?*

*For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.*

There are no automated integrated checks for accuracy. Information is verified manually by a processing agent visual inspection of requested submissions.

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

The system does not check for accuracy by accessing a commercial aggregator of information .

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

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

Budget and Accounting Act of 1950; General Accounting Office Title 8, Chapter #3; SSAN is used to index, and store pay affecting documents. Also, the use of the SSN is required from the customer for IRS tax reporting and cannot be eliminated. Camp Lejeune Project documents: Public Law 112-154 Title I Janey Ensminger Act which amends title 38, United States Code; 38 CFR Part 17 9/24/2014 Title 38, U.S.C. Chapter 3, Section 210 (c) (1), Title 38 U.S.C. 7301, 5 U.S.C. 552a.and Executive order 9397 Privacy Act of 1974 (5 USC 552a), Public Law 106-265 (FERC) and (P.L. 93-579). All information collected is required under the provisions of 31 U.S.C. 3322 and 31 CFR 210. This information will be used by the Treasury Department to transmit payment data, by electronic means to vendor's financial institution. Failure to provide the requested information may delay or prevent the receipt of payments through the Automated Clearing House Payment System.VA Financial Policy Vol 1 Chapter 4.

### **1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information**

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

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

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

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

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



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

Follow the format below when entering your risk assessment:

**Privacy Risk:**

Sensitive Personal Information may be released to unauthorized individuals.

**Mitigation:**

- DMS adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
- DMS relies on information previously collected by the VA from the individuals.
- Both VA contractors and VA employees are required to take Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training annually.
- File access granted only to those with a valid need to know and access privileges

**Section 2. Uses of the Information**

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Ensure individual is appropriate to receive benefits	Not used
SSN	Patient identifier	Not used
Phone Number	To contact the individual.	Not used
DOB	Identify patient age and confirm patient identity.	Not used
Mother’s Maiden Name	Verify spouse prior to marriage.	Not used
Personal Mailing Address	Verify individual known location	Not used
Personal Phone Number	Method to contact	Not used
Personal Fax Number	Method to send information electronically.	Not used
Personal Email Address	Another form of receiving correspondence	Not used
Financial Information	Show financial data projected to receive by individual	Not used

Account numbers (Health)	Communicate and bill third party health care plans.	Not used
Medications	Show prescriptions assigned to individual	Not used
Medical Records	Show individual history of illness and health issues.	Not used
Tax Identification Number	Identify tax payee.	Not used
Medical Record Number	Method to track individual records	Not used
Other Data Elements	Another form to identify patient who doesn't have SSN	Not used
Driver's License	Identify individual	Not used
Place of Birth	Confirm birth location	Not used
Business Telephone Number	Contact individual	Not used
Business Mailing Address	Send information	Not used
Business Email Address	Secondary means to contact individual.	Not used
Geographical Indicators	Determine a specific product origin	Not used
Medical Information	Confirm individual.	Not used

Medical Information: Used to confirm individual.

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

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

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

Retirement records: Paper correspondence from VA Central Business Office (CBO), Nationwide Payroll Structured Query Language (SQL) application, DMS, The Individual Retirement Record Close Out Data Capture Application (ICDC), Defense Finance and Accounting Service (DFAS) Remedy, Office of Financial Management Resources (OFMR), PAID, HRSmart, are all used in processing Federal Erroneous Retirement Coverage Corrections Act (FERCCA) cases and Administrative Retirement Corrections. If a correction to a previous retirement record is necessary, then a new record is created. The new record is archived in DMS Retirement Suite internal system. Corrections are forwarded to Office of Personnel Management so they can update their records. DFAS is notified if a post conversion correction is needed via (DFAS)

Remedy. Recertification: Information is used for tracking of requests and results of those requests. If new requests come in for a previously requested item, use stored library to search for items and status can be provided as needed. Audit of the Administrative and Loan Accounting (ALAC): Management analyzes the DMS data to ensure ALAC employees meet timeliness and accuracy standards and archiving documents for audit trail.

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

The system will maintain all new or previous information scanned or faxed pertaining to an individual. For correction or updates, a new record will be created and available to individuals or agencies to take actions.

### **2.3 How the information in the system is secured.**

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

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

All PII data are encrypted at rest and in transit.

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

No additional protections are implemented other than 2.3a response.

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

There is no SSN masking. However, there is segregation by roles across the eleven (11) DMS applications. Only specific users with certain security privileges have access to their department's SSN.

### **2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.**

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

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

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

Principle of Use Limitation: *Is the use of information contained in the system relevant to the mission of the project?*

*This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.*

2.4a *How is access to the PII determined?*

Access is determined based on he/she role and individual must complete appropriate training.

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

Yes

2.4c *Does access require manager approval?*

Yes

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

Monitored and tracked.

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

Data administrator and security

### Section 3. Retention of Information

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

#### 3.1 What information is retained?

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

Name  
Taxpayer Identification Name/SSN  
DOB  
Address  
Health Beneficiary Insurance Information Numbers  
Account numbers  
Vendor invoices for payment  
Treasury Schedule Number  
Check Number and Amount  
Payee Address  
Reason for Claim  
Document ID  
Phone number  
Email Address

Financial Account Information  
Current Medications  
Previous medical records  
Conditions/Illnesses  
Medical procedures and diagnoses  
Dates of Service of medical care  
Billed amounts for medical care  
Veteran sponsor information for CLFMP – including Name, SSN, DOB, gender, rank  
Mother's Maiden Name  
Phone Number  
Fax Number  
Any and all information relating to a VA Employee's career. (Retirement documents) SF -50's (Personnel actions) and Individual Retirement Records (IRR's)  
Payroll documents and scans

### 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 [vi](#)? This question is related to privacy control DM-2, Data Retention and Disposal.*

The following documents will be maintained for 56 years based on National Archivist and Records Administration (NARA) standards.

1. Direct Deposit Form (DDEFT)
2. TSP Saving Plan Printout (TSPSPP)
3. TSP 1 (TSP 1)
4. TSP 1 Catch-up (TSP1-C)
5. Transfer Between Agencies (TSP 19)
6. TSP Loans (TSPLN)
7. SF 1199 (SF 1199)
8. SF 1198 (SF 1198)
9. Savings Bond Elec. Form (SBEF)
10. TSP22 (TSP 22)
11. SF 50 (SF 50)
12. Record of Salary Payments (ROSPMT)
13. FEHB (SF 2809)
14. PAYROLL File Conversion (PRCONV)
15. Master RPO – Accessions and Separations (RPO)
16. Awards (AWD)
17. FEHB TFR (SF 2810)
18. Beneficiary Record (Bene)
19. Moving Expense (MOVEXP)
20. SF 2821 (FEGLI)

21. Military Service Deposit (MSD RPO)
22. Retirement Document (RETIRE)
23. Pay adjustments (PAYADJ)
24. Military Service Deposit App (MSD APP)
25. FEGLI election (SF 2817)
26. Recruitment Incentives (RECBON)
27. Student loan repayment (STULN)
28. Settlement Agreements (SETTLE)
29. Relocation, Recruitment, Retention Incentive (RRR)
30. SF 2803 (SF 2803)

The following document will be maintained for 15 years based on National Archivist and Records Administration (NARA) standards.

1. Workers Comp (WC)

The following documents will be maintained for 10 years based on National Archivist and Records Administration (NARA) standards.

1. W-4 (W4)
2. State Tax (STTAX)
3. City/county Taxes (LOCTAX)

The following documents will be maintained for 6 years based on National Archivist and Records Administration (NARA) standards.

1. Corrected Timecards (CORTC)
2. Leave Transfer (LVTFR)

The following documents will be maintained for 3 years based on National Archivist and Records Administration (NARA) standards.

1. Restored leave (RESLV)
2. Advanced sick leave (ADVSL)
3. Public Transit (TRANSIT)
4. SF1187/SF1188 (UNION)
5. CFC Contributions (CFCC)
6. Parking (PARKING)
7. Reserve duty/Active-duty orders (MILORD)
8. ADVANCE ANNUAL LEAVE (ADVAL)
9. Fitness Center (FIT)
10. SF1047 (PUBVOU)
11. SF 1187 (SF 1187)
12. Field Service Receipt (FSR)
13. SF 1188 (SF 1188)
14. Wage Garnishments (WAGGARN) after garnishment is terminated
15. Tax Levies (TAXLEV) after garnishment is terminated
16. Over Payment Record (OV) after garnishment is terminated
17. Bill of Collection (BOC) after garnishment is terminated
18. Child Support Agreements (CSA) after garnishment is terminated

The following documents will be maintained for 2 years based on National Archivist and Records Administration (NARA) standards.

1. Employment Verification Form (EMPVER)
2. Miscellaneous (MISC)
3. Change of Address Request (ADRCHG)
4. Separation Clearance Form (SEP\_CLR)
5. Wage and Separation (WAGSEP)
6. Request for Delivery of Salary Check (SALCHK)

The following document will be maintained for 4 months based on National Archivist and Records Administration (NARA) standards.

1. Savings Bonds (BONDS) after date of issuance of bond

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

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

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

Yes, GRS Schedule 1.1, Item #10, Disposition Authority DAA-GRS-2013-0003-0001  
<https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf>

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

All guidance is located at <https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf> under Records Management Regulations, Policy, and Guidance. GRS Schedule 1.1, Item #10, Disposition Authority DAA-GRS-2013-0003-0001

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

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

Electronic records are retained if required (GRS Schedule 1.1, Item #10), and are destroyed IAW (In Accordance With) NARA disposition instructions. Once physical paper file is scanned, digitized, and indexed for archival purposes, paper can be shredded after 6 months from scan date. This occurs on-site. FSC has contracted a records disposal company. 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

Version date: October 1, 2024

Page 15 of 36

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.

[https://www.va.gov/vapubs/search\\_action.cfm?dType=1](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.*

The DMS system does not permit “testing” to be conducted with PII.

### **3.6 PRIVACY IMPACT ASSESSMENT: Retention of information**

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

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

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

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

*Principle of Data Quality and Integrity: The PIA should describe policies and procedures for how PII that is no longer relevant and necessary is purged.*

*This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.*

Follow the format below:

#### **Privacy Risk:**

If DMS PII information is retained longer than identified in 3.2 then, users’ key information will be available if system is breached.

#### **Mitigation:**

Ensure data is purged according to time identified in 3.2 and check database frequently to confirm deletion to limit PII exposure.



## Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

### PII Mapping of Components

4.1a DMS consists of eight key components

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

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

*Internal Components Table*

<b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/ Storage of PII</b>	<b>Safeguards</b>
<b>OFMR</b>	<b>Yes</b>	<b>Yes</b>	<b>Outside DMS Boundary</b> • SSN • Date of Birth	<b>Payroll data reporting</b>	<b>Encrypted at rest and in transit</b>
<b>Offset</b>	<b>Yes</b>	<b>Yes</b>	<b>Outside DMS Boundary</b> • Tax Identification Number (TIN) • Telephone Number • Full Name	<b>Historical record and processing out-of-system financial requests</b>	<b>Encrypted at rest and in transit</b>
<b>NW Payroll</b>	<b>Yes</b>	<b>Yes</b>	<b>Outside DMS Boundary</b> • SSN • Full Name	<b>Payroll and retirement records processing</b>	<b>Encrypted at rest and in transit</b>

			<ul style="list-style-type: none"> <li>• Date of Birth</li> </ul>		
<b>ClaimsNet\$</b>	<b>Yes</b>	<b>Yes</b>	<ul style="list-style-type: none"> <li>• Full Name</li> <li>• Phone Number</li> <li>• Service dates</li> <li>• Email Address</li> <li>• Medical Record Number</li> <li>• Health Insurance Beneficiary Numbers</li> <li>• Maiden Name</li> <li>• Mother's Maiden Name</li> <li>• SSN</li> <li>• Tax Identification Number</li> <li>• Patient Identification Number</li> <li>• Address</li> <li>• Date of Birth</li> <li>• Place of Birth</li> <li>• Business Telephone Number</li> <li>• Business Mailing Address</li> <li>• Business Email Address</li> <li>• Geographical Indicators</li> </ul>	<b>Application of benefits and for payment of medical claims</b>	<b>Encrypted at rest and in transit</b>
<b>CMME9</b>	<b>Yes</b>	<b>Yes</b>	<ul style="list-style-type: none"> <li>• Name</li> <li>• SSN/TAX ID</li> <li>• Mailing Address</li> </ul>	<b>tracking retirement requests and results of</b>	<b>Encrypted at rest and in transit</b>

			<ul style="list-style-type: none"> <li>• Phone Number</li> <li>• Fax Number</li> <li>• Email address</li> <li>• Account Number</li> <li>• Financial Information</li> <li>• Business Telephone Number</li> <li>• Business Mailing Address</li> <li>• Business Email Address</li> </ul>	those requests	
IHSE9	Yes	Yes	<ul style="list-style-type: none"> <li>• Alien ID</li> <li>• Full Name</li> <li>• Tax Identification Number</li> </ul>	Application of benefits and for payment of medical claims.	Encrypted at rest and in transit
PAYE9	Yes	Yes	<ul style="list-style-type: none"> <li>• Full Name</li> <li>• Maiden Name</li> <li>• Mother's Maiden Name</li> <li>• Alias</li> <li>• SSN</li> <li>• Tax Identification Number</li> <li>• Patient Identification Number</li> <li>• Financial Account Number</li> <li>• Street Address</li> <li>• Email Address</li> </ul>	Batch, scan, and index paper documents received from business stations transitioning to FSC for payroll services	Encrypted at rest and in transit

			<ul style="list-style-type: none"> <li>• Personal Telephone Number</li> </ul>		
PRPC8_DMS	Yes	Yes	<ul style="list-style-type: none"> <li>• Name</li> <li>• Phone Number</li> <li>• SSN</li> <li>• Medical Record Number</li> <li>• Account</li> <li>• Patient Identification Number</li> </ul>	Business functions to validate travel documents, conduct historical	Encrypted at rest and in transit

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

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

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

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

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

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

Data Shared with Internal Organizations

<b>IT system and/or Program office. Information is shared/received with</b>	<b>List the purpose of the information being shared /received with the specified program office or IT system</b>	<b>List PII/PHI data elements shared/received/transmitted.</b>	<b>Describe the method of transmittal</b>
FSC/ FileNet	FSC repository for electronic documents	<ul style="list-style-type: none"> <li>• Name</li> <li>• Maiden Name</li> <li>• Mother's Maiden Name</li> <li>• Alias</li> <li>• Alien Identification/Registration Number</li> <li>• Home Address</li> <li>• Email Address</li> <li>• SSNs</li> <li>• TIN</li> <li>• Telephone Number</li> <li>• Fax Number</li> <li>• Business Telephone Number</li> <li>• Business Mailing Address</li> <li>• Business Email Address</li> <li>• Geographical Indicators</li> <li>• Date of Birth</li> <li>• Place of Birth</li> <li>• Taxpayer Identification</li> <li>• Vendor invoices for Payment Commercial payment information submitted by the vendor for payment purposes.</li> <li>• Financial Account Number - Banking Routing and Account Number</li> <li>• Patient Identification Number</li> <li>• Dates of Service</li> <li>• Medical Records Number</li> <li>• Health Insurance Beneficiary Numbers</li> <li>• Medical Procedures/Diagnosis</li> <li>• Medical Information</li> <li>• Health claims</li> </ul>	Web API (via https)
FSC/ VL Trader	Conduct internal audits	<ul style="list-style-type: none"> <li>• Name</li> <li>• SSN</li> <li>• DOB</li> <li>• Mother's Maiden Name</li> <li>• Personal Mailing Address</li> </ul>	sFTP

<b><i>IT system and/or Program office. Information is shared/received with</i></b>	<b><i>List the purpose of the information being shared /received with the specified program office or IT system</i></b>	<b><i>List PII/PHI data elements shared/received/transmitted.</i></b>	<b><i>Describe the method of transmittal</i></b>
		<ul style="list-style-type: none"> <li>• Personal Phone Numbers</li> <li>• Personal Fax</li> <li>• Personal Email Address</li> <li>• Financial Account Information Health Insurance Beneficiary Numbers/Account Numbers</li> <li>• Certificate/License Numbers</li> <li>• Current Medications</li> <li>• Previous Medical Records</li> <li>• Tax Identification Numbers</li> <li>• Other Unique Identifying Information</li> <li>• Driver's License</li> <li>• Place of Birth</li> <li>• Business Telephone Number</li> <li>• Business Mailing Address</li> <li>• Business Email Address</li> <li>• Geographical Indicators</li> </ul>	

**4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

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

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

Follow the format below:

**Privacy Risk:**

Privacy information may be released to unauthorized individuals.

**Mitigation:**

- DMS adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
- Both VA contractors and VA are required to take Privacy, HIPAA, and information security training annually.
- Information is shared in accordance with VA Handbook 6500
- File access granted

## Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

*Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.*

*This question is related to privacy control UL-2, Information Sharing with Third Parties*

### Data Shared with External Organizations

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

Version date: October 1, 2024

## **5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

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

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

*Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.*

*Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

*This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing*

Follow the format below:

### **Privacy Risk:**

There is no external sharing.

### **Mitigation:**

There is no external sharing.

## **Section 6. Notice**

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

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

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

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

DMS does not collect PII/PHI information directly from individuals. However, the systems that use DMS may have individuals that submit their information directly to VA on the OMB 10091 form in order to receive payment from the government.

SORN Used:1.



<https://www.govinfo.gov/content/pkg/FR-2023-08-31/pdf/2023-18807.pdf>

Individuals Submitting Invoices - Vouchers for Payment -VA (13VA047).

*6.1b If notice was not provided, explain why.*

DMS does not collect PII/PHI information directly from individuals therefore, a notice will not be provided.

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

See 6.1b response.

**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.*

Declining consent to provide the information may result in not processing of financial transactions, and denial of payment or benefits. Payments will not be paid unless information is obtained and used to process the payment or financial transactions. Individuals do not have to provide all the requested information for the purpose of establishing eligibility for the Camp Lejeune Family Member Program, it may delay or result in denial of your request for Camp Lejeune Family Member Program benefits. Failure to furnish the requested information will have no adverse impact on any other VA benefit to which you may be entitled.

**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.*

If an individual wish to remove consent for a particular use of their information, they should contact the nearest VA Regional office, a list of where it can be found at:  
<http://benefits.va.gov/benefits/offices.asp>.

**6.4 PRIVACY IMPACT ASSESSMENT: Notice**

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

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

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

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must ensure that information is used only for the purpose articulated in the notice.

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

Follow the format below:

**Privacy Risk:**

Privacy information could potentially be collected prior to providing the written notice.

**Mitigation:**

- DMS does not collect information directly from Veterans, detainees, or their families. This is done within other systems ATO's, and these systems have responsibility for notification per their system policy. DMS only provides a user interface to access the information provided.
- Information is used only to process payments and determine eligibility for the program.
- Payments will not be paid unless information is obtained and used to process the payment.

## Section 7. Access, Redress, and Correction

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

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

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

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

*DMS does not collect PII/PHI information directly from individuals. Nevertheless, individuals may access their information via Freedom of Information Act (FOIA) and Privacy Act procedures. VA employees may access their information by contacting their servicing HR office or local payroll office.*

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

The system is not exempt 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?

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.*

Veterans can correct/update their information online via the VA's eBenefits website. <http://benefits.va.gov/benefits/offices.asp> VA employees may access their information by contacting their servicing HR office. Camp Lejeune Program: Contact CLFMP Help desk 1-866-372-1144, Retirement Records: In the event a retirement correction is necessary, CBO is notified to decide on the type of correction and if it is FERCCA or NON-FERCCA. Consolidated Patient Account Center (CPAC) stations will contact Enterprise Content Manager team via email to have the record corrected. Audit of the Administrative and Loan Accounting (ALAC): returns any inaccurate or erroneous information / documentation to the Regional Office for correction.

## 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.*

Camp Lejeune Program: Contact CLFMP Help desk 1-866-372-1144 will provide the information needed. Retirement Records: The employee is notified by mail. If determined to be a FERCCA, and if there is an election opportunity, the employee is allowed to make a choice/election as to which retirement system they want to be in. If the employee is not allowed to make an election, then they are notified of CBO's decision, and that the decision is final and cannot be appealed.

## 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.*

DMS does not collect PII/PHI information directly from individuals. Nevertheless, Veterans can correct/update their information online via the VA's eBenefits website.

<http://benefits.va.gov/benefits/offices.asp>

## **7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction**

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

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

*Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.*

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

*Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.*

*This question is related to privacy control IP-3, Redress.*

Follow the format below:

### **Privacy Risk:**

- Inaccurate data may be used during processing.

### **Mitigation:**

- Individuals do not have direct access to the DMS systems. However, they can correct information by contacting each of the business units.

## **Section 8. Technical Access and Security**

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

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

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

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

Individuals must take and pass training on Privacy, HIPAA, information security, and government ethics. Individuals must have a completed security investigation. Once training and the security investigation are complete, a request is submitted for access before access is granted; this request must be approved by the supervisor, information owner, and OIT.

*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?*

No other agencies have access to system.

*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.*

Read only

Regular users have access to view all properties /View content/ Annotation/ Read permissions/ Add/Edit Markups)

Supervisors have access to view all properties /View content/ Annotation/Modify all Properties/Delete)

Listing of all roles in DMS

LGY User

AAD User

Audit User

Station User

ALAC Manager

FSC Payroll Super User

FSC Payroll User Station Payroll HR Super User

Station Payroll HR User

Station Payroll HR Nationwide User

FSC Scanning User

CPAC Site Admin

CPAC FSC Coordinator

CPAC FSC Indexer

CPAC Reviewer

CPAC View Only User

CPAC FSC Rescan

Payment Resolution Role

Payment Resolution

Recertification Indexing Role

Vendorizing Manager

Vendorizing Tier 1 User

Vendorizing Tier 2 User

Accounting User 1

Accounting User 2

Accounting User 3

## **8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.**

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

No. Contractors must take and pass training on Privacy, HIPAA, information security, and government ethics.

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

Yes. Contractors will have access to the system and their contracts are reviewed on an annual basis.

8.2c. What involvement will contractors have with the design and maintenance of the system?

Contractors designed and implemented the DMS system. Also, contractors are responsible for maintaining and performing annual maintenance to keep the system running properly.

### **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.*

Privacy and Information Security Awareness and Rules of Behavior (TMS course # 10176) is required for all Federal and Contractor personnel that require access to the VA Network. Annual training compliance is closely monitored. Other required Talent Management System courses monitored for compliance: VA 10203: Privacy and HIPAA Training VA 3812493: Annual Government Ethics.

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

8.4a If Yes, provide:

1. *The Security Plan Status: Approved*
2. *The System Security Plan Status Date: August 14, 2023*
3. *The Authorization Status: Authority to Operate*
4. *The Authorization Date: Granted October 12, 2023*
5. *The Authorization Termination Date: October 12, 2025*
6. *The Risk Review Completion Date: October 12, 2023*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): High*

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 not completed or In Process, provide your **Initial Operating Capability (IOC) date**.  
N/A

## Section 9 – Technology Usage

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

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

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

No. This section is not applicable as DMS does not use cloud technology.

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

No. This section is not applicable as DMS does not use cloud technology.

### 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.*

No. This section is not applicable as DMS does not use cloud technology.

### 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.*

No. This section is not applicable as DMS does not use cloud technology.

**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. This section is not applicable as DMS does not use RPA technology.



## Section 10. References

### Summary of Privacy Controls by Family

#### *Summary of Privacy Controls by Family*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

**Signature of Responsible Officials**

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

---

**Privacy Officer, Morla Roberts**

---

**Information Systems Security Officer, Ronald Murray**

---

**Information Systems Owner, Jonathan M. Lindow**

## APPENDIX A-6.1

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

**HELPFUL LINKS:**

**[Records Control Schedule 10-1 \(va.gov\)](#)**

**General Records Schedule**

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

**National Archives (Federal Records Management):**

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

**VA Publications:**

<https://www.va.gov/vapubs/>

**VA Privacy Service Privacy Hub:**

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

**Notice of Privacy Practice (NOPP):**

VHA Directive 1605.04

[IB 10-163p \(va.gov\)](#)