Privacy Impact Assessment for the VA IT System called:

Salesforce – Medical Disability Examination Office Invoice Validation Tool (MDEO IVT)

Veterans Benefits Administration

Medical Disability Examination Office (MDEO) eMASS ID # 2128

Date PIA submitted for review:

4/18/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lakisha Wright	Lakisha.Wright@va.gov	202-632-7216
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000 x4613
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

Salesforce-Medical Disability Examination Office Invoice Validation Tool (MDEO IVT) is a Salesforce module that is designed to streamline, validate, and audit MDE vendor invoices. The tool will allow for increased efficiency in reviewing invoices, analyzing trends, and conducting vendor invoice audits that are performed by the Medical Disability Examination Office team.

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. What is the IT system name and the name of the program office that owns the IT system?

"Salesforce: Medical Disability Examination Office Invoice Validation Tool (MDEO IVT)" is owned by Medical Disability Examination Office. Salesforce Government Cloud Plus (SFGCP) manages in collaboration between Veterans Affairs Central Office (VACO) Information Technology Support Service's (ITSS), Access Management/VA Business Owners and Office of Information Technology (OIT).

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

Salesforce- Medical Disability Examination Office Invoice Validation Tool (MDEO IVT) is a Salesforce module that is designed to streamline, validate, and audit vendor invoices. The tool will allow for increased efficiency in reviewing invoices, analyzing trends, and conducting invoice audits that are performed by the Medical Disability Examination Office (MDEO) team.

The Salesforce- Medical Disability Examination Office Invoice Validation Tool will be utilized by the Medical Disability Examination Office team in reviewing invoices submitted for payment by Medical Disability Examination (MDE) vendors. A monthly upload of invoice(s), in the format of a Microsoft Excel file, is provided by each vendor. The invoice file contains veteran information such as the name, partial address information (town, state and zip code), file number (which may contain the Social Security Number (SSN)), disability examination type and date the disability examination was conducted. The data from the invoice is then reviewed, reconciled, and validated by the Medical Disability Examination Office team to allow for the creation of an analytics dashboard and reports for team and leadership review.

The system has internal connections to Master Person Index (MPI), ID.me, and Corporate Database (CRP). The purpose for each connection is as follows: MPI - identifying the Veteran and Veteran related information, ID.me - access for vendors for monthly upload of invoices, Corporate Database (CRP) - to maintain a database of the medical disability examinations being invoiced for Veterans.

C. Who is the owner or control of the IT system or project?

MDEO is the business owner. The Digital Transformation Center (DTC) manages the Salesforce IT Contractor supporting the development/integration. DTC will sustain the system on behalf of MDEO.

2. Information Collection and Sharing

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

The MDEO IVT platform will be utilized by about 120 users consisting of MDEO team members and vendors. Users are authenticated and allowed access into the tool using Single Sign On (SSO) two-factor authentication or ID.me. User login and access is monitored to MDEO IVT tool.

The number of Veterans whose information is stored in the system is currently over 3 million Veterans per fiscal year.

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

The IT system is used to manage MDE Vendor Invoices. The information includes a list of the disability benefits questionnaires and ancillary procedures (e.g., labs, tests, etc.) that were completed for each Veteran in support of the medical disability examinations that the MDE Vendors are requesting payment for.

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

The Salesforce- Medical Disability Evaluation Office Invoice Validation Tool (MDEO IVT) is a Salesforce system for invoice validation. MDEO IVT validates that Disability Benefit Questionnaires (DBQ) medical exam documentation and lab documents have been filed in Veteran Benefits Management System (VBMS) (which is a source of data for the Enterprise Data Warehouse (EDW)) to correspond with a vendor billing line. Vendors upload invoices into the MDEO Salesforce environment which triggers a validation of the invoice file. One of the many validations of this file is to check the Enterprise Data Warehouse to verify the existence of these Disability Benefit Questionnaires and Lab documents.

G. Is 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 single system will be utilized by MDEO IVT users within VBACO. The system is hosted on the VA Salesforce platform.

3. Legal Authority and SORN

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

The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12. Individuals Submitting Invoices- Vouchers for Payment-VA- 13VA047/88FR60269 2023-18807.pdf (govinfo.gov)

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?

This PIA for MDEO IVT will not

- Affect the relevant SORN applicable for the system is "Individuals Submitting Invoices- Vouchers for Payment-VA- 13VA047/88FR60269 2023-18807.pdf (govinfo.gov).

4. System Changes

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

This PIA for MDEO IVT will not

- Cause any business processes to change,
- Affect the relevant SORN applicable for the system is "Individuals Submitting Invoices- Vouchers for Payment-VA- 13VA047/88FR60269 2023-18807.pdf (govinfo.gov).

K. *Will the completion of this PIA could potentially result in technology changes?*

New integrations which include MuleSoft as a middleware will result in technological changes to PIA for MDEO IVT.

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. It must also match the information provided in question 3.4 of the PTA.

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

- ☒ Name
- ☐ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address (PARTIAL)
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements: Veteran File Number (may contain SSN), type of disability examination of veteran, date of medical disability examination, vendor name, vendor contract number, examiner name, examiner state, examiner license number, examiner unique national provider identifier (NPI)

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

PII Mapping of Components (Servers/Database)

Salesforce- Medical Disability Examination Office Invoice Validation Tool (MDEO IVT) consists of four 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 MDEO IVT 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 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
VA – Master Person Index (VA-MPI)	**Yes**	**Yes**	Veteran Name, Address, DOB, File number may contain SSN	Perform MDE Vendor Invoice Validation, Salesforce Requirement	Encrypted transmission
ID.me	**Yes**	**Yes**	Vendor first and last name, address and federation ID	Perform MDE Vendor Invoice Validation, Salesforce Requirement	Single Sign On-external through encrypted transmission
Corporate Databases (CRP)	**Yes**	**Yes**	Veteran First and Last Name, Veteran File Number (may contain SSN)	Perform MDE Vendor Invoice Validation	Protected behind VA firewall, with limited access to those that need to know
Veterans Benefits Administration – Enterprise Data Warehouse (EDW)	**Yes**	**Yes**	Veteran File Number (may contain SSN), Veteran Name	Perform MDE Vendor Invoice Validation	Protected behind VA firewall, with limited access to those that need to know

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 information is collected by the MDE Vendors that have invoiced for the medical disability examination services performed for Veteran(s) benefits determination.

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.
The information is a monthly aggregate from MDE Vendors that have invoiced for the services they performed for Veteran(s) benefits determination.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
Vendors contracting with Medical Disability Examination Office (MDEO) upload monthly invoices into MDEO IVT tool. The file containing Veteran information and type of service rendered is then validated by MDEO team.

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?
On a monthly basis, vendors access the MDEO IVT platform using SSO to upload an excel file(s) containing medical disability examinations provided to Veterans. This information is then validated by the MDEO team to process the payment of invoices.

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?
This is not applicable for MDE OIVT.

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.
MDEO IVT does not make any decisions about any individual. MDEO IVT is a system that assists MDEO in validating vendor invoices only. The system includes validation to check invoice data submitted by vendors.

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?
Veteran information is validated real-time with MPI system. Dependent information will be validated individually by VA employees. VA employee users will then review individually the invoices and submit it to their supervisor for approval prior to the invoice being finalized and approved.

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 the Title 38 U.S.C. 5106.

The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12. Individuals Submitting Invoices- Vouchers for Payment-VA- 13VA047/88FR60269 2023-18807.pdf (govinfo.gov)

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: 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: The risk is associated with the collection of PII information on the Veteran. The information is collected to provide service of reviewing the invoices uploaded by the vendors.

Mitigation: Veteran information required to process the invoices serviced by the vendors in contract with the VA are collected. The information for the veteran is matched real-time with the Master Person Index. Additional evaluation and validation is done by VA employees having access to the tool prior to processing the payment to the vendors.

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
Veteran First and Last Name	Used to identify the Veteran for which the medical disability examination was performed	Not used
Veteran File Number	Unique identifier of the Veteran to validate invoicing	Not used
Partial address	Location of the medical disability examination services provided to the Veteran used for invoice validation	Not used
Type of DBQ/Diagnosis	The type of Disability Benefit Questionnaire and/or Diagnostic performed used for invoice validation	Not used
Date of Service	The actual date of the medical disability examination or ancillary diagnostic was performed used for invoice validation	Not used
Vendor Name	The vendor that has invoiced for the services provided used for invoice validation	Not used
Vendor Contract Number	MDE Vendor Contract Number associated with the medical disability examination services provided used for invoice validation	Not used
Examiner Name	The examiner who performed the medical disability examination or ancillary service used for invoice validation	Not used
Examiner State	State where the examiner is licensed and provided service	Not used

	(license state can be more than one) used for invoice validation	
Examiner License	Examiners' State License Number in the state where service was provided for invoice validation	Not used
Examiner Unique National Provider Identifier (NPI)	Unique provider identifier used to validate invoices	Not used

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?
MDEO IVT is the tool that will be utilized to analyze the Invoice Data submitted by vendors. The validation is built into the system to replace manual review of invoice data.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
Salesforce reporting dashboards are used to review and validate invoices, analyze trends over time and across vendors, conduct audits and for increased oversight for senior leadership and reporting metrics. The system does not make create any information on an individual. It's used for MDEO Vendor invoice validation only.

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?
MDEO IVT is accessed via a secured webpage utilizing Single Sign On (SSO) technology. MDEO IVT is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there. The data exchange will be through a site-to-site encryption having Transmission Layer Security. Salesforce Shield Product provides FIPS 140-2 certified encryption.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
Fields such as SSN are protected by Salesforce Shield Protect which provides FIPS 140-2 certified encryption. The SORN Federal Case Management Tool (FCMT) – VA 202VA005Q. (2021-26257.pdf (govinfo.gov)) defines the information collected from veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a veteran's benefits, such as compensation or education.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
MDEO IVT is accessed via a secured webpage utilizing SSO technology. MDEO IVT is implemented with the required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.
Additionally, Privacy Officer, Information System Security Officer, and Information System Owner will be responsible for maintaining all safeguards are put in place to protect PII and other sensitive information.

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?
Users are provided access to PII only on a need-to-know basis to execute/ facilitate a work tracking request within the MDEO IVT application. Profile based settings is applicable to the tool limiting the type of information accessed by individual users. Additionally, the SORN defines the use of the information and how the information is accessed, contained, and stored in the system.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?
Access to the MDEO IVT system is requested by the employee's supervisor and approved by the system owner through DTC. All users will be required to authenticate to the system with a PIV card and will only have permissions to perform their assigned function. Based upon that function, each user will only have access to information on those participants which are assigned

to them by their manager. The system will perform extensive logging to detail all actions taken by a user. Some of these actions are (but not limited to):
1) Logon / Logoff
2) Create Data
3) Update Data
4) Delete Data

2.4c Does access require manager approval?
Yes, supervisor/manager approval is required for new users accessing MDEO IVT application.

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

Profile-based setting available in Salesforce is leveraged for users access in MDEO IVT application. User have limited access to PII information captured in the tool and access is monitored using logging details available through Salesforce cloud technology.

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

Salesforce MDEO IVT is accessed via a secured webpage utilizing SSO technology. SF-MDEO IVT is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there. Accessibility to data is granted based on the permission sets and profile-based settings is applied based on FedRAMP Salesforce Gov Cloud Plus platform. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card and/or Access VA. Single Sign On external (SSOe) is used to provide credential access to VA modules/communities residing in the Salesforce application, the determinant of access is organizational affiliation rather than personal identity. For some module(s) the required organizational e-mail confirmation and multi-factor authentication (MFA) will be enforced (IAL1), but no identity proofing (IAL2) and vice versa. The managers will reject any applications from individuals who do not work with them, do not require access, or are not using the correct e-mail address.
Additionally, The MDEOIVT Privacy Officer, Information System Security Officer, and Information System Owner will be responsible for maintaining all safeguards are put in place to protect PII and other sensitive information.

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*

MDEO IVT, a Salesforce module, retains information of Veterans and Members of Public such as: First and Last Name, Veteran File Number (which may contain Social Security Number (SSN)), partial address (town, state, zip code), Type of DBQ/Diagnostic, date of medical disability examination service, vendor name, vendor contract number, examiner name, examiner state, examiner license, examiner unique national provider identifier (NPI).

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.*

The information is retained following the policies and schedules of VA's Records management Service and NARA in "VBA Records Control Schedule, VB-1, Part II & VBA Records Control Schedule, VB-1, Part I.

Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting. Item number: 4000.1.b. Disposition instructions: Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use or destroy when business use ceases. DAA-GRS-2013-0003- 0001. Item 010 and item 011.

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?

No – MDEO will determine the retention period. Records shall not be removed or destroyed.

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

MDEO does not want a destruction or removal of data schedule. Removal of information will be an MDEO decision as there are contractual implications.

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.

MDEOIVT tool adheres to the VBA Records Control Schedule, VB-1, Part II & VBA Records Control Schedule, VB-1, Part I

All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500. (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.

MDEO IVT does not use PII information of the users stored in this application for research, testing or training. Users accessing the tool would have to undergo basic Privacy training such as, Privacy and Information Security Awareness and Rules of Behavior and information security training annually.

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 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:

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

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

Follow the format below:

Privacy Risk: The retention of PII and SPI information of the Veterans and members of the public pertaining to vendor specific information until MDEO determines the data is no longer required to be retained is at risk of exposure to unauthorized disclosure.

Mitigation: Longer retention times are at risk of unauthorized exposure. All data at rest within the SFGCP security boundary is encrypted in accordance with FIPS 140-2, as well as protected by FedRAMP certified "HIGH" security controls. Use of FedRAMP HIGH controls implemented under the FedRAMP ATO. Collectively, these controls within the SFGCP security boundary provide maximum protection to all VA Salesforce data.

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***
Office of Information and Technology | VA-Master Person Index (VA- MPI)	Validation of vendor invoices	Veteran Name, Address, DOB, File number may contain SSN	Site-to-Site Encrypted Transmission
Enterprise Program Management Office | ID.me	Validation of vendor invoices	Vendor first and last name, address and federation ID	Single Sign On-external through encrypted transmission
Benefits Integration and Administration | Corporate Database (CRP)	Validation of vendor invoices	Veteran First and Last Name, Veteran File Number, Compensation	Site-to-Site Encrypted Transmission

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*
Vendor Excel File	Validation of vendor invoices	Veteran Name, Veteran File Number (which may contain Social Security Number (SSN)), Partial Address (Town, State, Zip Code), Type of Disability examination, Date of medical disability examination or ancillary diagnostic, Vendor Name, Vendor Contract Name, Examiner name, Examiner License Number, Examiner Unique National Provider Number (NPI)	Monthly upload of the excel file to SF- MDEO IVT through MuleSoft site-to-site encryption

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: Without appropriate security controls, PII information shared internally may result in unauthorized data access.

Mitigation: Release of PII to unauthorized individuals is prohibited by the Privacy standards mandated to all VA employees, affiliates, trainees, volunteers, and contractors. Both contractor and VA employees are required to take Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training annually. Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system. Monthly upload of files by the vendors will be authenticated using ID.me. Encrypted site-to-site transcription. Data and files are encrypted both in transit and at rest. User specific, user access data configured for each role category and on least privilege base.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

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: Not applicable for this tool.

Mitigation: Not applicable for this tool.

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.

The SORNs defines the information collected from Veterans and Members of Public, use of the information, and how the information is accessed and stored.
Federal Case Management Tool (FCMT) – VA 202VA005Q.
(https://www.govinfo.gov/content/pkg/FR-2021-12-03/pdf/2021-26257.pdf)

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

Not Applicable.

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.

Veterans are notified by MDEO Vendors when contacted for medical disability examination services.

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.

No, this is not applicable for the MDEO IVT tool. A monthly invoice file containing Veteran information and services performed by the MDE vendors are uploaded into the tool. This is then reviewed and validated by VA employees on the MDEO team.

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.

This is not applicable for the tool. Vendors upload the file containing Veteran and services performed by MDE Vendors. The contract between the MDEO Vendors and MDEO office covers the consent of services performed in support of Veteran Medical Disability Examinations.

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 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 Transparency: Has sufficient notice been provided to the individual?

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

Privacy Risk: Risk is associated with Veteran being unaware their information is being shared and stored within MDEO IVT system.

Mitigation: Veterans are informed by the MDE Vendor that their information is shared with the VA. VA authorized MDE Vendors to perform medical disability examination services for Veterans.

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.***

Veterans are not given access and have no right to know what MDE Vendors are requesting VBA invoice payments for nor the associated price. That information is contract proprietary information. The SORN provides access procedure as follows,

Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing. System Manager: Paul Zeien, Director—Education Veterans Readiness and Employment Product Line—EVREPL (FCMT), Office of Information & Technology, Department of Veterans Affairs, 5000 S 5th Avenue, Hines, IL 60141 (708) 483– 5432 and Paul.Zeien@va.gov. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

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)?

SF-MDEOIVT is not exempt from 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?

Veterans do not have access to the information received by the MDEO team in invoices. Vendors with incorrect invoices will be able to re-submit the corrected invoice for validation and approval. Each incorrect invoices will be processed as per the contract agreement.

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.

Vendors re-submit the corrected information if the invoice submitted is incorrect. The correction on inaccurate information is then reviewed by the VA employee users having access to the MDEO IVT tool to validate invoice accurately.

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.

Notification to vendors follows the same process as 7.1. - Veterans do not have access to the information received by the MDEO team. Vendors with incorrect invoices will be able to re-submit the corrected invoice for validation and approval. Each incorrect invoices will be processed as per the contract agreement.

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.

No formal redress is provided. Alternative to correction follows the same process of 7.1- Veterans do not have access to the information received by the MDEO team. Vendors with incorrect invoices will be able to re-submit the corrected invoice for validation and approval. Each incorrect invoices will be processed as per the contract agreement.

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: The individuals cannot access, redress or correct their information captured in the MDEO IVT e-invoices. MDE Vendors correct invoice information following the process in the contract.

Mitigation: Veterans can NOT request the vendors to share the particular use of their information being shared with the MDEO IVT.

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?

Yes, new users access the system with supervisor/managerial approval. User roles identify the information and applications a user can access. To receive access to the system, another user of with appropriate permissions must sponsor them. The sponsor will describe which applications the user needs to access, the user's role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level control of the information and data.

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?

DTC VA Contractor support teams possess privileged users responsible for maintaining the system on behalf of the VA. VA role-based security training is required for all privileged users of VA systems. Single sign-on utilizing VA PIV cards and/or Citrix VPN (over contractor laptops and unsecure networks) will be required.

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.

MDEO users have various levels of access for MDEO IVT depending on their role. Some users have higher access to perform specific validation duties, analyze trends, etc. Other users only have read-only access to look up invoice information.

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.

Yes, contractors will have access to the MDEO IVT platform to upload the invoices. A vendor has access to upload the file on a monthly basis through authentication by ID.ME. BAA is in place between the MDE vendors and MDEO office.

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.

General Training includes, VA Privacy and Information Security Awareness and Rules of Behavior, TMS 10203 - Privacy and Health Insurance Portability and Accountability Act (HIPAA), VA On-Boarding enterprise-wide training, and annual information security training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date: 1/25/2023*
3. *The Authorization Status:* Active
4. *The Authorization Date:* 7/17/2023
5. *The Authorization Termination Date: 7/17/2026*
6. *The Risk Review Completion Date:* 9/19/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
This is not applicable.

Section 9 – Technology Usage

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

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

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

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)*

Yes, MDEO IVT utilizes Salesforce Gov Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus. MuleSoft middleware integration allows dataflow through different systems.

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.*

Yes, VA has full ownership of the PII that will be shared through the MDEO IVT platform. Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B.

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.

Ancillary data is not collected by MDEO IVT. VA has full ownership over the data stored in the VA Lighthouse API support system.

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.

VA has full authority over data stored in Salesforce - Medical Disability Examination Office Invoice Validation Tool.

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).

MDEO IVT does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

LAKISHA WRIGHT

Digitally signed by LAKISHA WRIGHT
Date: 2024.09.27 11:03:18 -04'00'

Privacy Officer, Lakisha Wright

JAMES BORING

Digitally signed by JAMES BORING
Date: 2024.09.26 13:15:48 -04'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2024.09.26 11:25:55 -04'00'

Information System Owner, Michael Domanski

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).

OPRM website for SORN: https://www.oprm.va.gov/privacy/systems_of_records.as
Federal Case Management Tool (FCMT) (202VA005Q) - 2021-26257.pdf (govinfo.gov)

VA Directive 6500: VA Publication

The Privacy Act of 1974 , set forth at 5 U.S.C. 552a

Federal Regulation: 38 CFR 1.579.

31 CFR § 1.32 - Use and disclosure of social security

HELPFUL LINKS:

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 Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices