Privacy Impact Assessment for the VA IT System called:

Privacy Act Automation/Disclosure.AI - DAI

Veterans Benefits Administration (VBA)

Office of Mission Support

2491

Date PIA submitted for review:

5/2/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Chiquita Dixson	Chiquita.dixson@va.gov	202-632-8923
Information System Security Officer (ISSO)	Joseph Guillory	Joseph.guillory@va.gov	619-204-6840
Information System Owner	Simon Caines	simon.caines@va.gov	202-461-9468

Abstract

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

The DAI system is a modular, multi-tenant service delivery platform empowering rapid iterative deployment of AI (Artificial Intelligence) and Automation technologies. This managed service system is designed to provide a range of tools and services, including Robotic Process of Automation (RPA) and intelligent Optical Character Recognition (iOCR) capabilities, as well as redaction functionalities. It offers the VBA both current and future opportunities for use cases and technologies, thereby enhancing its Privacy Act Automation Managed Service. Specifically, the system streamlines and automates the VBA's process for responding to Privacy Act requests, providing an efficient and effective solution for managing sensitive information.

DAI integrates with the following systems, VBMS, Caseflow, VBA Data Warehouse (VD2), SSOi and FOIAXpress to identify the documents relevant to a Privacy Act request (e.g., DD214), then apply VBA's redaction policies and guidelines, and provide a portal to allow the Requester to access the redacted documents. VBA Privacy Act Automation Managed Service Solution is hosted on AWS East Commercial FedRamp ready and is comprised of workflow steps to allow for quality assurance and approval by VBA personnel in addition to the following components:

Automation Integration – The Automation and Integration module is run using UiPath RPA software with 2 RPA software components; Orchestrator and Robots.

Intake and Decision – The Intake and Decision module uses these main components Intelligent Character Recognition, Natural Language Processing, and Human-in-the-Loop (HITL).

Redact, Review, and Release (R3) – SecureRelease is a Deloitte product built on Relativity platform which does the following: redact engine, review engine, and release engine.

AI4RR – Artificial Intelligence for Records Review is a Deloitte AI product which does the following: Intake records - digitalize and validate via intelligent optical character recognition (IOCR), Language understanding - NLU and AI Algorithms locate keywords, Automation Engine - understands business context and natural language to align content with policy and data with reporting, Processing Documentation – tags and rates policy evidence and potential fraud or abuse and Centralized Portal - tags data in real time, sends notifications, manages workflow.

Business Intelligence (BI) Service – BI dashboards are built using AWS QuickSight which is a cloud-native AWS dashboarding tool.

AWS Cloud Native Services – AWS tools and services used by the DAI system.

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?

IT System: Privacy Act Automation/Disclosure.AI – DAI
Program Office: Office of Mission Support

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

DAI integrates with the following systems, VBMS, Caseflow, and FOIAXpress to identify the documents relevant to a Privacy Act Request (e.g., DD214), then apply VBA's redaction policies and guidelines, and provide a portal to allow the Requester to access the redacted documents.

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

Deloitte LLP

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?

DAI expects the number of individual's information that will be stored to be over 100,000. DAI does not collect information from front end users but utilizes information collected through interconnection with 3 (VBMS, Caseflow, FOIAXpress) VA systems to process and output privacy act requests for users.

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

Privacy Act Automation/Disclosure.AI (DAI) is designed to provide an automated function to VBA's manual process of responding to Privacy Act requests. DAI is a modular, multi-tenant service delivery platform empowering rapid iterative deployment of AI (Artificial Intelligence) and Automation technologies. This managed service system is designed to provide a range of tools and services, including Robotic Process of Automation (RPA) and intelligent Optical Character Recognition (iOCR) capabilities, as well as redaction functionalities. It offers VBA both current and future opportunities for use cases and technologies, thereby enhancing its Privacy Act Automation capabilities to reduce VBA's backlog and fulfill its mission. The system will integrate with the following systems: VBMS Cloud Assessing, Caseflow, and FOIAXpress Assessing to identify the documents relevant to a Privacy Act request (e.g., DD214), then apply VBA's redaction policies and guidelines, and provide a portal to allow the requestor to access the redacted documents.

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

DAI is comprised of six components:
Automation Integration – The Automation and Integration module is run using UiPath RPA software with 2 RPA software components; Orchestrator and Robots.

Intake and Decision – The Intake and Decision module uses these main components Intelligent Character Recognition, Natural Language Processing, and Human-in-the-Loop (HITL).

Redact, Review, and Release (R3) – SecureRelease is a Deloitte product built on Relativity platform which does the following: redact engine, review engine, and release engine.

AI4RR – Artificial Intelligence for Records Review is a Deloitte AI product which does the following: Intake records - digitalize and validate via intelligent optical character recognition (IOCR), Language understanding - NLU and AI Algorithms locate keywords, Automation Engine - understands business context and natural language to align content with policy and data with reporting, Processing Documentation – tags and rates policy evidence and potential fraud or abuse and Centralized Portal - tags data in real time, sends notifications, manages workflow.

Business Intelligence (BI) Service – BI dashboards are built using AWS QuickSight which is a cloud-native AWS dashboarding tool.

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?

N/A – DAI system is hosted on AWS US East - Northern Virginia (Availability Zones: AZ1, AZ2)

3. Legal Authority and SORN

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

The DAI system has the authority for the collection of VA and Veteran data through interconnection of VA systems for the purpose of the outlined system is as follows:
HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R) Part 164, Standards for Privacy of Individual Identifiable Health Information
Privacy Act of 1974
58VA21/22/28 - Compensation, Pension, Education and Vocation Rehabilitations and Employment Records
Confidentiality of Certain Medical Records, 38 U.S.C
Federal Information Security Management Act (FISMA)

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?

The system is not being modified currently, in addition, the SORN covers usage of cloud technology.

4. System Changes

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

No

K. Will the completion of this PIA could potentially result in technology changes?
No

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
- ☒ 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)

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

Other PII/PHI data elements:

Social Security Number (Doctors / Medical Professional)
Work Phone
Work Email
Personal Health Information (PHI) – (Service Treatment Records / Compensation and Pension Exams)

PII Mapping of Components (Servers/Database)

Privacy Act Automation/Disclosure.AI consists of 3 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 Privacy Act Automation/Disclosure.AI 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**
smartext: AIEE-SMARTEXT-PRD-SQL01	Yes	Yes	First Name Middle Name Last Name Date of Birth Personal Address Personal e-mail address Phone numbers Social Security Number Personal Health Information (PHI)	Ingested from VBMS, Caseflow and FOIAXpress information systems as part of required information needed to process privacy act request	Encryption of data in motion and Data at rest

			Social Security Number (Doctors / Medical Professional)		
smartext: AIEE-SMARTEXT-PROCESSING-PRD-MYSQL01	Yes	Yes	First Name Middle Name Last Name Date of Birth Personal Address Personal e-mail address Phone numbers Social Security Number Personal Health Information (PHI) Social Security Number (Doctors / Medical Professional)	Ingested from VBMS, Caseflow and FOIAXpress information systems as part of required information needed to process privacy act request	Encryption of data in motion and Data at rest
VAPAAPSRDB01	Yes	Yes	First Name Middle Name Last Name Date of Birth Personal Address Personal e-mail address Phone numbers Social Security Number Personal Health	Ingested from VBMS, Caseflow and FOIAXpress information systems as part of required information needed to process privacy act request	Encryption of data in motion and Data at rest

			Information (PHI) Social Security Number (Doctors / Medical Professional)		

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?

DAI sources of PII and PHI collected from VA systems are:

- VBMS Cloud Assessing
- FOIAXpress
- Caseflow

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.

VBMS Cloud Assessing, FOIAXpress and Caseflow provided DAI with Privacy Act requests, workflows, and PHI and PII data needed by DAI to process and redact Privacy Act request output.

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

DAI system provides dashboard reports that covers the total number of requests processed, types of requests, how long for a request to be processed and other general system metrics. The dashboard reports do not contain any PII or PHI data or data elements.

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?

DAI dataflow is initiated when DAI system pulls privacy requests letters in pdf formats from three externally connected VA systems: Caseflow, VBMS Assessing, and FOIAXpress, through an AES 256-bit encrypted VPN tunnel established between the (VA TIC) and the (D2C2, use FedRAMP name) hosted Palo Alto firewall.

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?

The system does not collect information on a form. The system ingests veteran's records based on their Privacy Act request, and then redacts the required information before the records are then made available to the veteran.

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

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

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

Information accuracy is accomplished through utilizing a human in the loop process to validate data for the redactions of the records function of the system. That is records that a veteran request, will be pulled into DAI from VBMS. The system will use its built-in machine learning to redact the records, and then the internal Deloitte team will review to make sure that the system did it correctly. Before the Deloitte review process records are routed to a VA team for them to QA. Deloitte team reviews first, then the VA QA team, after the records are published to the portal for the veteran to retrieve.

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 use commercial aggregators to check for accuracy.

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 DAI system has the authority for the collection of VA and Veteran data through interconnection of VA systems for the purpose of the outlined system is as follows:
HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R) Part 164, Standards for Privacy of Individual Identifiable Health Information
Privacy Act of 1974

58VA21/22/28 - Compensation, Pension, Education and Vocation Rehabilitations and Employment Records
Confidentiality of Certain Medical Records, 38 U.S.C
Federal Information Security Management Act (FISMA)

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: Veteran's data is retrieved, processed, and stored in the DAI system during Privacy Act request processing. DAI's operations team has access to the system which could lead to unintended exposure of veteran's data to systems/individuals that do not have a need or authority to access such data due to system error or a malicious actor.

Mitigation: DAI has implemented security controls and procedures to prevent unauthorized access to Veteran data including:

- Cisco DUO Multifactor Authentication (MFA)
- Microsoft Secure MFA
- Separation of Duties
- Use of least privilege for granting access to the information system

Additionally, DAI employees undergo a Rules of behavior (RoB) training which they sign at completion, indicating adherence to the privacy of information they may come across while doing their job.

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's Name, Veteran's Date of Birth, Veteran's Social Security Number, Veteran's phone number, Veteran's email, Veteran's address Social Security Number (Doctors / Medical Professional) Work Phone Work Email Personal Health Information (PHI) – (Service Treatment Records / Compensation and Pension Exams)	Used to process Privacy Act requests from external VA clients.	Used to output Privacy Act request results after appropriate redactions are applied.

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?

The types of data retrieved and processed by DAI information system include Veteran's Name, Veteran's Date of Birth, Veteran's Social Security Number, Veteran's phone number, Veteran's email, Veteran's medical records, Veteran's gender.
DAI system utilizes AWS Quicksight for business intelligence analysis for dashboard reports to VBA.

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 DAI system does not create or make available new or previously unutilized information about veterans. Veterans can only request records that already exist and are available from the VA.

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?

The DAI system does not create or make available new or previously unutilized information about veterans. Veterans can only request records that already exist and are available from the VA.

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

DAI utilizes redaction functions to protect veterans' social security numbers along with TLS 1.2 with AES 256-bit encryption for transmitting data and AES 256-bit encryption for storage.

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

DAI defines all sensitive, classified, and non-publicly available information as information that requires encryption. These are encrypted via AWS Key Management Service (KMS) or Microsoft Internet Information Services (IIS) server, which are FIPS 140-2 compliant.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII/PHI is protected via documented Access control – utilizing the principle of least privilege requiring role-based permissions for administrative access – which requires approval. Additionally, access, use and modification of information/data is monitored via audit logging and monitoring processes. Security events are collected and stored for a year and logs are kept in long term storage for seven years, per NARA requirements.

Prior to approval for account creation and onboarding – all users must complete requirements such as: Privacy and HIPAA training (TMS#: VA 10203), VA Privacy and Information Security Awareness and Rules of Behavior training (TMS#: VA 10176), AIEE OpenCloud Role-Based Training (Deloitte), AIEE Platform Role Based Training (Deloitte) and AIEE OpenCloud Rules of Behavior (Deloitte).

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

DAI documents and implements access control policies and procedures; the access control policy and procedure documents address DAI users' responsibilities regarding the system. The implemented Access control for the DAI is well documented in the approved System Security plan.

2.4c Does access require manager approval?

DAI access is based on the principle of least privilege and are role based. Access requires approval before access is granted.

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

Access to PII is protected by access controls and modification of information/data is monitored via audit logging and monitoring processes.

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

DAI Operations Team

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
The types of date retrieved, processed, and retained by the information system includes:
Veteran's Name,
Veteran's Date of Birth,
Veteran's Social Security Number, Veteran's phone number,

Veteran's email,
Veteran's address
Social Security Number (Doctors / Medical Professional)
Work Phone
Work Email
Personal Health Information (PHI) – (Service Treatment Records / Compensation and Pension Exams)

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.*

All records generated from processing of a privacy request is retained for 5 years per contractual requirements at which point records are to be turned over to the VA. All records are electronic and access to records are granted through a portal for the privacy act requester. To guarantee the integrity and completeness of the record DAI utilize access restrictions and industry encryption standards for data at rest and data in transit for all privacy records.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

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

Yes

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

National Archives and Records Administration General Record Schedule 4.2: Information Access and Protection Records - Access and Disclosure Request Files
36 CFR Part 1236, Electronic Records Management

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.

DAI system adheres SPI elimination procedures such as collecting minimum data required for fulfilling business purposes and retaining PII data required for transactional and audit purposes and transactional usage. DAI follows Privacy Act (PA) regulations that require DAI to retain all privacy act request responsive records for a period of five years following delivery to the requester.

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.

DAI system does not use the information/data collected for research, testing or training.

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: PII data is only required for transactional and audit purposes and transactional usage and should only be retained for five years following delivery to the requester for transactional purposes, keeping data past the required period and use creates unnecessary use and unintended exposure to users that may not need to have access to such PII data.

Mitigation: DAI has implemented data handling procedures to take care of transactional uses of data and audit usage. For data in transactional state – Access control methods including MFA and Virtual access control are in place to ensure that only authorized DAI users that have gone through the background check and security and compliance training and required to have access to the DAI system could potentially have access to Privacy data. All DAI contractors are required to sign a non-disclosure agreement. Policies and procedures such as data archiving or disposal are also in place to guide the use of auditable 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***
VBMS Cloud Assessing	DAI receives Privacy Act Request and data required to process	First Name Middle Name Last Name	VPN Tunnels established via MOU/ISA

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*
		Date of Birth Personal Address Personal e-mail address Personal Phone numbers Social Security Number Personal Health Information (PHI) – (Service Treatment Records / Compensation and Pension Exams) Social Security Number (Doctors / Medical Professional) Work E-mail address	
FOIAXpress Assessing	DAI receives Privacy Act Request and data required to process	First Name Middle Name Last Name Date of Birth Personal Address Personal e-mail address Personal Phone numbers Social Security Number Personal Health Information (PHI) – (Service Treatment Records / Compensation and Pension Exams) Social Security Number (Doctors / Medical Professional) Work E-mail Address	VPN Tunnels established via MOU/ISA
Caseflow	DAI receives Privacy Act Request and data required to process	First Name Middle Name Last Name Date of Birth Personal Address Personal e-mail address Personal Phone numbers Social Security Number Personal Health Information (PHI) – (Service Treatment Records / Compensation and Pension Exams)	VPN Tunnels established via MOU/ISA

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*
		Social Security Number (Doctors / Medical Professional) Work E-mail address	
VBA Data Warehouse (VD2)	DAI is interconnected to VBA Data Warehouse to provide request completion updates and retain records of all completed privacy requests.	First Name Middle Name Last Name Date of Birth Personal Address Personal e-mail address Personal Phone numbers Social Security Number Personal Health Information (PHI) – (Service Treatment Records / Compensation and Pension Exams) Social Security Number (Doctors / Medical Professional) Work E-mail Address	VPN Tunnels established via MOU/ISA
Identity and Access Management Assessing	DAI connects to SSOi for access control resources that establish identity and authentication and PIV use services on the DAI system.	Access Controls configurations for identity and authentication service	VPN Tunnels established via MOU/ISA

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: Unintended exposure of PII/PHI data to personnel that should not have access to VA data.

Mitigation: Data sharing between DAI and the three interconnected VA systems is done securely and DAI will have MOU/ISAs in place which guides the transfer of data.

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***
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

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 DAI does not interconnect with any other external systems, only VA systems.

Mitigation: Not Applicable DAI does not interconnect with any other external systems, only VA systems.

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.

Not Applicable, DAI does not do any collection of information or data directly from Veteran users.

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

Notice is not provided by the DAI system, as the records requests that the DAI system processes are pulled from VBMS, not from the individual requestor, and then the applicable records are redacted and provided to the requestor.

Please provide response here

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.

Not Applicable DAI does not do any collection of information or data directly from Veteran users.

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.

Not Applicable DAI does not do any collection of information or data directly from Veteran users.

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.

Not Applicable DAI does not do any collection of information or data directly from Veteran users.

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

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

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

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

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

Privacy Risk: Not Applicable DAI does not do any collection of information or data directly from Veteran users.

Mitigation: Not Applicable DAI does not do any collection of information or data directly from Veteran users.

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.***

DAI utilizes a public facing veterans' portal that requires authentication by front end VA customer users to access processed privacy act request. The portal discloses VA privacy act laws and system usage laws provided to veterans and for their acknowledgement before accessing the portal.

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)?

DAI is not exempt from access provision of privacy act. DAI system provides a public facing portal for veteran users to access their processed privacy request.

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?

DAI is a privacy act system with the function of processing and outputting privacy act requests quickly for VA customers.

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.

DAI system process privacy request with records that exist, and the system does not provide a capability for amending records or redress.

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.

DAI system process privacy request with records that exist, and system does not provide a capability for amending records.

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.

DAI system process privacy request with records that exist, and the system does not provide a capability for amending records.

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: DAI provides access processed privacy act request for VA customers. The DAI system does not provide the capability for redress or corrections because privacy requests are processed from existing records. There is privacy risk because of access to records on a public facing portal.

Mitigation: DAI utilizes authentication controls for access to the portal the includes usernames and passwords, MFA and initial credentials needed to access the portal is provided through mail all part of defense in depth mechanism to list the exposure of risk.

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?

DAI has documented Access Control policies in place to ensure that only authorized users can access the system. DAI has privileged accounts and has implemented Role Based Access Control (RBAC) and least privilege principles which limit the system use to only authorized users and DAI system users are only provided privileges required to perform their given task. For users to gain access to the DAI system, they must go through an onboarding process which includes background check and security awareness training and rules of behavior training.

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?

Users from other agencies do not have access to the DAI 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.

DAI only utilize privileged roles for the different users in the system and are granted privilege access according to their roles and responsibilities.

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.

DAI system is a managed service information system maintained by Deloitte LLP. The DAI system supports Veteran Benefits Administration - benefits integration

administration under the portfolio of benefit and memorial service for the office of mission support. DAI requires all contractors prior to gaining access to the system to sign a Non-Disclosure Agreement (NDA) and complete a criminal background check.

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

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

All DAI system users are required to take annual security training including the following: Privacy and HIPAA training (TMS#: VA 10203), VA Privacy and Information Security Awareness and Rules of Behavior training (TMS#: VA 10176), AIEE OpenCloud Role-Based Training (Deloitte), AIEE Platform Role Based Training (Deloitte) and AIEE OpenCloud Rules of Behavior (Deloitte).

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

8.4a If Yes, provide:

1. *The Security Plan Status:* DAI SSP will be generated out of eMASS with completion of step 3.
2. *The System Security Plan Status Date:* TBD
3. *The Authorization Status:* DAI is going through its first initial ATO process.
4. *The Authorization Date:* TBD
5. *The Authorization Termination Date:* TBD
6. *The Risk Review Completion Date:* DAI is going through its first initial ATO process.
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.***

June 30, 2024

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)*

DAI is hosted on Amazon Web Service (AWS) commercial cloud US East-1 Northern Virginia AZ1 & AZ2 with the failover AWS US West-2 Oregon AZ1 & AZ2 – FedRamp Ready

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.*

Section B.2 of DAI Amendment of Solicitation/Modification of Contract 36C10E23Q0029 0002 between DAI and the VA outlines; "Federal law and regulations, including the Federal Acquisition Regulations (FAR), shall govern this Contract/Order. …In the event of conflict between this clause and any provision in the Contract/Order or the commercial license agreement or elsewhere, the terms of this clause shall prevail. The Contractor shall deliver to the Government all data first produced under this Contract/Order with unlimited rights as defined by FAR 52.227-14."

DAI and AWS data ownership follows the section 6 Proprietary Right of the AWS Customer Agreement linked where AWS does not have any rights to end user data, which would include any VA data processed on the DAI system.

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.

The CSP does not collect or have access to veterans' data.

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.

The AWS Shared Responsibility model states that the customer is responsible for security of the data in the cloud embedded in contracts with AWS and DAI.

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).

DAI will use RPA agents to automate routine tasks involved in the processing of privacy act requests for the DAI system. All RPA solutions will be deployed locally and operate in an unattended mode. DAI will be using RPA primarily to 1) automate the collection of data needed to complete a privacy request 2) redact information that is not required to be included in the privacy request output 3) finalize and present the privacy request in readable text for the external user on the veterans' portal.

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**

ID	Privacy Controls
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.

CHIQUITA DIXSON

Digitally signed by CHIQUITA DIXSON
Date: 2024.05.21 08:49:57 -04'00'

Privacy Officer, Chiquita Dixson

JOSEPH GUILLORY

Digitally signed by JOSEPH GUILLORY
Date: 2024.05.23 10:53:54 -07'00'

Information System Security Officer, Joseph Guillory

SIMON CAINES

Digitally signed by SIMON CAINES
Date: 2024.05.17 14:11:38 -04'00'

Information System Owner, Simon Caines

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:

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