Privacy Impact Assessment for the VA IT System called:

Caseflow Assessing

Board of Veterans Appeals (BVA)

Veterans Affairs Central Office

eMASS ID #753

Date PIA submitted for review:

November 14, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kary Charlebois	Kary.Charlebois@va.gov	202-382-2906
Information System Security Officer (ISSO)	Griselda Gallegos	Griselda.Gallegos@va.gov	512-326-6037
Information System Owner	Jason Rhinehart	Jason.Rhinehart@va.gov	610-529-6125

Abstract

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

Caseflow is a web-based system that will iteratively and ultimately replace the Veterans Appeals Control and Locator System (VACOLS) as the system of record for appeals. Caseflow will provide functionality to the Board of Veterans' Appeals and other departments/stakeholders to enable the processing and tracking of appeals and related processes. The system will leverage integrations with VA systems to provide functionality that improves the efficiency of processing appeals, working with information/documents, responding to business needs/requests (e.g., FOIA), and updating central data as applicable in source systems.

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?

Caseflow Assessing owned by the Board of Veterans Affairs (BVA) Office of Technology and Information.

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

Caseflow will provide functionality to the Board of Veterans' Appeals and other departments/stakeholders to enable the processing and tracking of appeals and related processes.

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

Caseflow is a web-based system that will iteratively and ultimately replace the Veterans Appeals Control and Locator System (VACOLS) as the system of record for appeals.

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 VACOLS system maintains more than 1.6 million Veteran's appeals information.

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

Caseflow will store any information related to the processing of an appeal that is not currently stored by other systems at the VA such as specific appeal details, appeal history, status, appeal process metrics, etc.

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

- Caseflow **Certification** ensures that appeals are transferred accurately from VBA to the Board, eliminating the risk of lost appeals and reducing the rate of mismatched errors. Validates that VACOLS and VBMS document dates match.

- Caseflow **Dispatch** creates End Product work items for the processing of Board decisions to help to prevent delays, ensure consistency, and track appeals. Additionally, it facilitates the transfer of cases back to the Area of Jurisdiction (AOJ) or specialty centers for adjustment, following the issuance of a decision by the Board of Veteran Appeals (BVA)

- Caseflow **eFolder Express** allows a user to bulk-download documents from a Veteran's eFolder, thereby eliminating the need to manually click and save these documents one by one. As a Veteran's eFolder can contain anywhere from hundreds to thousands of documents, eFolder Express is greatly reducing time spent on reviewing Veteran's appeals and processing FOIA and Privacy Act requests.

- Caseflow **Hearing Prep** helps judges to prepare for their hearings more quickly all within one application. It allows judges to view their upcoming hearings, transfer hearing worksheets between judges and attorneys, view relevant appellant information, take notes before and during a hearing, and review documents in the Veteran's eFolder.

- Caseflow **Reader** allows all documents in a Veteran or claimant's case to be read and annotated in a single window. Additionally, the tool allows users to organize documents using categories, issue tags, and comments from multiple users, thereby streamlining the case review process.

- Caseflow **Intake** will start off as a pilot proof of concept to immediately support the tracking of incoming Rapid Appeals Management Process (RAMP) opt-in letters. The application guides ARC Claims Assistants through the process of updating the necessary systems and creating the End Product in VBMS.

- Caseflow **Queue** will manage, and track legacy and Appeals Modernization Act (AMA) appeals through the appeals process. "Who does what, and when" for appeals. Appeals are currently processed at the Board of Veterans' Appeals (BVA) using VACOLS. There will be a variety of queues that will allow work to flow to the correct user needing to carry out tasks. Such queues are Judge, Attorney, Co-located, and VSO.

- Caseflow **Hearing Schedule** supports the Board of Veterans' Appeals ability to schedule hearings under the legacy system and under the Appeals Modernization Act. It creates automated ways to build aspects of the hearing schedule, allows Board staff to view and filter the entire hearing schedule, and edit individual aspects of the schedule. With more than 80,000 Veterans waiting for hearings, this functionality will enable the Board to identify which Veterans should be scheduled for hearings and where they should be scheduled.

- Caseflow **API** backend application programming interface (API) allows other VA systems to viewdata pertaining to a Veteran's appeal status. It will tell a comprehensive story about an

appeal. It includes data about the history of the appeal, its status, dynamic time estimates for the next steps, alerts about needed actions, and descriptions of the issues on an appeal and their disposition. This data makes the Board's docket visible showing exactly where a Veteran is in line, including the specific number of appeals ahead of them. This information provides a progress towards a decision, even when the wait might last years. This API is currently consumed by Vets.gov, our first user.

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?

With Caseflow being hosted on AWS GovCloud, it is in one location. However, it leverages the cloud computing infrastructure capabilities provided by AWS to establish replicated storage sites within AWS regions retaining redundancy of the system and data including all security controls for quick recovery of system information.

3. Legal Authority and SORN

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

Caseflow will operate under authority from Title 38 of the United States Code and Title 38 of the Code of Federal Regulations. 2023-14569.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?

Caseflow does not have a SORN in progress that needs to be modified or require approval.

4. System Changes

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

The Caseflow system currently has an Authority to Operate (ATO) which requires the completion of a PIA. Additionally, this PIA will not result in any technology changes nor will it in any circumstances require changes to business processes.

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

Additionally, this PIA will not result in any technology changes nor will it in any circumstances require changes to business processes.

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.

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)

Other:

- Health Insurance Beneficiary Numbers
- Certificate/License numbers (Medical/Occupational)
- Vehicle License Plate Number

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

- Integration Control Number (ICN)
- Attorney Elections
- Veteran Appeal Information
- Veteran Claim Information
- Veteran Health Information
- Incoming/outgoing correspondence related to benefits claims
- Incoming/outgoing correspondence metadata related to benefits claims
- Previous Medical Records
- Benefits Request Issue
- Participant ID
- Place of Birth
- Birth Sex
- Date of Death

PII Mapping of Components (Servers/Database)

Caseflow consists of six 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 Caseflow 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**
Caseflow-certification	Yes	Yes	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information,	BVA Judges need to prepare for hearings.	Multi-factor authentication and data encryption

			Veteran Claim Information, Veteran Health Information		
Redshift-Prod	Yes	Yes	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	Reporting Data Warehouse for Board of Veteran Appeals	Multi-factor authentication and data encryption
Caseflow Extract Transform Load (ETL)	Yes	Yes	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	Reporting Data Warehouse for Board of Veteran Appeals	Multi-factor authentication and data encryption
efolder_express	Yes	Yes	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information,	Efolder Metadata for documents used in the remediation of Veteran Appeals	Multi-factor authentication and data encryption

			Veteran Claim Information, Veteran Health Information		
Redshift-Prodtest	Yes	Yes	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information Veteran Claim Information, Veteran Health Information	Reporting Data Warehouse for Board of Veteran Appeals	Multi-factor authentication and data encryption
Prod-vacols-dr	Yes	Yes	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information Veteran Claim Information, Veteran Health Information	Replicated staging database for legacy appeals.	Multi-factor authentication and data encryption

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?

As noted in the overview, Caseflow collects data from BGS, VBMS, VVA, and VACOLS as needed to both enable and assist in the completion of appeals related workflows.

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.

Caseflow will leverage data that already exists at the VA and update source systems to avoid unnecessary duplication when possible. The requirements for data are driven by the goal of providing Veterans with resolution of appeals and inquiries.

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

N/A

1.3 How is the information collected?

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

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

Information is internally generated/input by Caseflow users in support of the appeals process or obtained via electronic transmission from the systems described in section 1.2. Furthermore, incoming correspondence will drive the required processes. For example, a notice from a Veteran providing a new mailing address will result in an update to this information in the system.

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?

N/A

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.

If possible, information in the system is retrieved from the VA systems stated in question 1.2. However, for some of that information, we allow users to correct any incorrect data, should they have reason to do so.

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?

When integrating with source data and permitted, Caseflow will update these systems in support of reducing incorrect or outdated data. Caseflow will also leverage automation and connections with other systems, when possible, to improve accuracy. For example, in Caseflow Certification, we cross-reference data in VACOLS and VBMS to assure accuracy. This automatic accuracy verification is one of the main benefits of Caseflow Certification.

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

Following is the list legal authority for Caseflow system to operate:

- Veterans Appellate Records System (VARS) (44VA01)
- VA Handbooks on Records Management Procedures (6300.1-6300.8)
- The Privacy Act of 1974, 5 U.S.C. § 552a.
- Veteran's Benefits - Rules and Regulations (Title 38 of the United States Code, Sections 501(a))

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

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: Access to a Veteran's efolder presents a significant privacy risk due to Veterans' PHI and PII information.

Mitigation: We are employing multiple strategies to minimize the risk of this access. First, only the personnel that need to access the eFolder in this way will have access to eFolder Express (attorneys, FOIA officers, and support/RO staff as required). These personal are already trusted with Veterans' eFolder's and have taken the appropriate privacy trainings. Secondly, our system will only allow a user to view or download documents at his/her security sensitivity level. The user will receive and error message if he/she attempt to view or download documents with a sensitivity level greater than his/hers.

For further measures and monitoring, the system logs access and activity.

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	Identification purposes	Not used
Social security number	Identification purposes	Not used
Birth date	Identification purposes	Not used
Mother's maiden name	Identification purposes	Not used
Mailing Address	Used to contact individual	Not used
Zip Code	Used to contact individual	Not used
Phone Numbers	Used to contact individual	Not used
Fax Numbers	Used to contact individual	Not used
Email Address	Used to contact individual	Not used
Emergency Contact Information (Name, phone, etc.)	Used to contact individual	Not used
Financial Account Information	Used for benefits disbursement	Not used
Health Insurance Beneficiary and Account Numbers	Used for benefits disbursement	Not used
Certificates/License Numbers	Used to manage Bar Accreditation	Not used
Vehicle License Plate Number	Parking privileges	Not used
Internet Protocol (IP) Address Numbers	Account management	Not used
Previous Medications	Medical History	Not used

Current Medications	Medical History	Not used
Race/Ethnicity	Medical History	Not used
Incoming/outgoing correspondence related to benefits claims	Used to contact individual	Not used
Incoming/outgoing correspondence metadata related to benefits claims	Used for benefits disbursement	Not used
Veteran records	Used for benefits disbursement / Medical History	Not used
Spouse's name	Beneficiary information	Not used
Child's name	Beneficiary information	Not used
Gender	Beneficiary information	Not used
Birth Sex	Beneficiary information	
Spouse's date of birth	Beneficiary information	Not used
Child's date of birth	Beneficiary information	Not used
Place of Birth	Beneficiary information	Not used
Integration Control Number (ICN)	Used for benefits disbursement	Not used
Veteran Appeal Information	Used for benefits disbursement	Not used
Veteran Claim Information	Used for benefits disbursement	Not used
Veteran Health Information	Medical History	Not used
Benefits Request Issue	Used for benefits disbursement	Not used
Participant ID	Used for benefits disbursement	Not used
Date of Death	Beneficiary information	Not used
Attorney Elections	Used for benefits disbursement	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?
The most common data and source analyzed is the Veteran's efolder which hold the record of an appellant's appeal. The Veteran's efolder is used by the Board of Veteran's Appeals to adjudicate appeals, as well as, fulfilling FOIA requests and other business needs. The various components of Caseflow are tools used to analyze data. Other sources of analysis lie in the comparison of content between other VA systems, such as VACOLS and VBMS. Caseflow Intake, Dispatch, and Certification are examples of tools that do various types of data comparisons between these systems. The Caseflow performs analyzes on data relevant to the appeals process such as matching, relational analysis, and reporting. This can be seen in:

- Metric dashboards showing the total number of data items that have been and are being processed for a given day, week, month, or fiscal year. Such as, the total number of RAMP Elections Sent, RAMP Elections Received, RAMP Elections Processed, and

RAMP Refiling Received for Intake and total number of Establish Claim Tasks Identified from VACOLS, Establish Claim Task Activity, Establish Claim Task Completion Rate, Time to Claim Establishment, Establish Claim Tasks Canceled, Establish Claim Tasks with Decisions Uploaded to VBMS for Dispatch. No new or previously unutilized information about an individual is created or made available.

- Document date comparisons between systems (VACOLS and VBMS) providing discrepancy data and next step tasks, such as Decision date. This can trigger the addition of a new document in the Veteran's efolder allowing the appeals process to continue. This creates and makes available new information about an individual.
- Creation of End Products in other systems (VBMS) to track additional work that needs to be completed based on the findings, such as where an appeal needs to be re-routed for additional information. If additional information is needed, it will be added to the Veteran's efolder allowing the appeals process to continue. This has the potential of causing the creation and making available new information about an individual.
- Available documents comparisons between VA systems (VACOLS and VBMS) or within a specific VA system (VBMS) producing discrepancy data and next step tasks, such documents include Decisions, Notice of Disagreement, various VA Forms, End Products. This can trigger the addition of a new document in the Veteran's efolder allowing the appeals process to continue. This creates and makes available new information about an individual.
- Task ordering for appeals processing, such as AOD having priority processing. This will allow for the appeal decision to be generated sooner for the veteran and be added to their eFolder continuing appeals process. This creates and makes available new information about an individual.

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.

Data discrepancies found in some of the analysis identified above are updated in the appropriate VA system. Authorized VA employees process Veteran appeal claims will be able to view and act appropriately on updated or add information.

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?

Caseflow data in transit uses Transport Layer Security (TLS) which encrypts internet traffic of all types.

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

Caseflow has enabled encryptions for all PII data in transit and at rest.

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

For safeguards, to ensure, Caseflow has three levels of user access (increasing privilege order): typical user, manager& system admin. Access is granted with a CSEM application request and users are required to complete all levels of approval which include the Information Security Officer (ISO) as final approver. Caseflow also uses 2 factor authentication for all application access. Caseflow EBS Volume production ec2 are encrypted for data at rest. The Redshift instances are also encrypted at rest.

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?

Only VA personnel who have been authorized to process Veteran health benefits or appeal claims will have access to Caseflow. Additionally, to ensure that a user only sees the allowed PII, specific roles and functions have been implemented using Common Security Employee Manager (CSEM).

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

This authorization is determined first by the Caseflow Product team who define the use of the product.

2.4c Does access require manager approval?

This is done in conjunction with a user's supervisor who has identified him/her as needing access to Caseflow to perform his/her daily tasks. All users are required to complete and provide evidence of the VA Privacy and Security training.

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

All these controls and procedures are documented and monitored by the Caseflow Project Management team. Additional controls include those described in section 1.7 to mitigate privacy risks.

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

Only VA personnel who have been authorized to process Veteran health benefits or appeal claims will have access to Caseflow. Additionally, to ensure that a user only sees the allowed PII, specific roles and functions have been implemented using Common Security Employee Manager (CSEM). This authorization is determined first by the Caseflow Product team who define the use of the product. This is done in conjunction with a user's supervisor who has identified him/her as needing access to Caseflow to perform his/her daily tasks. All users are required to complete and provide evidence of the VA Privacy and Security training.

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 system retains, for varying lengths of time, information that is required to support the processing and tracking of appeals and related activities as described in the overview as well as in support of developing/maintain the system. Following list identifies the data retained within Caseflow.

Veteran's Name / Appellants Name, Social security number, Birth date, Financial Account Information

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.*

Any new data created in Caseflow will be stored according to existing retention schedules (indefinite). For any data pulled from other VA systems, Caseflow relies on the retention schedules of those systems such as BGS, VBMS, and VACOLS. Please review SORN for Retention information SORN from the OPRM site **(https://department.va.gov/privacy/). SORN Identifier – (44VA01 / 88 FR 44185- Veterans Appellate Records System-VA"** 2023-14569.pdf (govinfo.gov)

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?

Following are the relevant Record Control Schedules (RCS) Job Authority defining the retention schedule:
General Records Schedules (GRS) | National Archives
Medical Administration Service Records – N1-015-87-004
Veterans Benefits Administration (VBA) Records - N1-015-90-001
Veterans Medical Records Folder –N1-015-90-005
Perpetual Medical Files -N1-015-91-007
Electronic Patient Medical Record -N1-015-02-00

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.

In accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1, all Caseflow data is electronically stored in a database. At the end of the retention period, a Rails stored procedure will be executed to permanently delete all data records from the main and backup application databases. Any data files that may have been copied to a user's personal computer is automatically detected and deleted by Caseflow system functionality on regular intervals (every 72 hours upon log in) This functionality ensure data remains current and provides a method for disposal of expired data.
(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.

Caseflow has developed a replicated web-based system that is in a demo environment. This system is used for research, testing, and training. The PII data contained in the system is all dummy data and doesn't represent real people or information.

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: There is a risk that information could be retained for longer than necessary.

Mitigation: Since a Veteran's efolder and information can potentially be updated frequently and Caseflow retrieves this data from other VA systems, Caseflow repeatedly refreshes of any necessary data that may have been retained. Timeframes for updating this data varies anywhere from instantly to 2 hours or 2 days depending on the data element.

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?

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***
Board of Veterans' Appeals (BVA)	For processing and tracking appeals.	First name Last name Birth Date, SSN, Veteran Address, Attorney Elections	use SSL over TCP database connections
Freedom of Information Act (FOIA) Office and offices responding to FOIA/Privacy Act and related requests (including Office of General Council)	For fulfilling FOIA/Privacy Act and related requests	First name Last name Birth Date, SSN, Veteran Address Incoming/outgoing correspondence related to benefits claims Incoming/outgoing correspondence metadata related to benefits claims	Electronically -**REST** over HTTPS using SSL encryption and Certificate exchange
Veteran Benefits Information (VBA) (including Regional Office (RO) Certifying Officials) and other VA employees/contractors supporting appeals	For supporting claims that are appealed	First name Last name Birth Date, SSN, Veteran Address, Attorney Elections, Benefits Request Issue. & Same data elements of Caseflow-Certification, ETL Caseflow & VACOLS.	Electronically –**REST** over HTTPS using SSL encryption and Certificate exchange

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*
processing and tracking			
VA Systems (including BEP, Veteran Benefits Management System (VBMS), Benefit Gateway Services (BGS), Veterans Appeals Control and Location System (VACOLS), Vets.gov)	For processing and tracking appeals	First name Last name Birth Date, SSN, Veteran Address, Attorney Elections, Benefits Request Issue.	**BGS** - SOAP over HTTPS using SSL encryption and Certificate exchange VACOLS - use SSL over TCP database connections **VBMS -** SOAP over HTTPS using SSL encryption and Certificate exchange
VA offices that require access to appeals data (including Veterans Health Administration, VBA Performance Analysis and Integrity (PA&I), BVA)	For processing and tracking appeals and for reporting (congressional and otherwise)	First name Last name Birth Date, SSN, Veteran Address, Attorney Elections, Benefits Request Issue.	Use SSL over TCP database connections
VBA - Veterans Benefits Administration - **Tableau**	Internal Reporting system. Tableau uses - Personally, Identifiable Information (PII)	First name Last name Birth Date, SSN, Veteran Address, Attorney Elections, Benefits Request Issue. & Same data elements of Caseflow-Certification, ETL Caseflow & VACOLS.	use SSL over TCP database connections
Board of Veterans Appeals - **Redshift Prod**	AWS redshift database cluster is a data warehouse. Provide Personally Identifiable Information PII data	Same data elements of Caseflow_certification, Caseflow ETL & VACOLS	use SSL over both TCP and HTTPS.

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
	elements to Tableau.		
Board of Veterans Appeals - **Redshift PreProd**	TIB Team will be performing data transformation work on pre-production environment (snapshot of Caseflow production data) which is used for official reporting to the Board. The quality and accuracy of the data is primarily TIB Teams responsibility	Same data elements of Caseflow_certification, Caseflow ETL & VACOLS	use SSL over TCP database connections
Board of Veterans Appeals - Caseflow	Read only access to the ARMS and TIB Team	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	use SSL over TCP database connections (port 443)
Board of Veterans Appeals	Hosts the Production Dynamic Task Hierarchy webserver . Display the Appeals ID information for BVA	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	use SSL over TCP database connections (port 443)
Board of Veterans Appeals	Hosts the ProdTest Dynamic Task Hierarchy Webserver in the Production VPC. Display the Appeals ID information for BVA	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	use SSL over TCP database connections (port 443)
Board of Veterans Appeals	TIB Team will be performing data transformation work on the Data pulled	First name Last name Birth Date, SSN,	use SSL over TCP database connections (port 443)

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*
	from Aurora Caseflow PostgreSQL replica database which is in Caseflow VPC to Production DB installed in ARMS VPC.	Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	
Board of Veterans Appeals	TIB Team will be performing data transformation work on the Data pulled from Aurora Caseflow PostgreSQL replica database which is in Caseflow VPC to PreProd DB installed in ARMS VPC.	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	Use SSL over TCP database connection
Board of Veterans Appeals - Tableau	TIB Team will be reading Aurora Caseflow PostgreSQL replica data to ARMS Tableau Prod Server for reporting purposes that's in ARMS Prod VPC.	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	Use SSL over TCP database connection
Board of Veterans Appeals - Tableau	TIB Team will be reading Aurora Caseflow PostgreSQL replica data to ARMS Tableau PreProd Server for reporting purposes that's in ARMS Prod VPC	First name Last name Birth Date, SSN, Veteran Address, Veteran Appeal Information, Veteran Claim Information, Veteran Health Information	Use SSL over TCP database connection
Identity and Access Management (IAM) – VA Master Person Index	VA MPI shall support Search for Person (Attended, Returning Corresponding IDs)	First name Last name Date of birth ICN SSN Participant ID	SOAP over TLS. Caseflow transmits First name, Last name, Date of

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*
	requests from Caseflow.	Gender Place of birth Birth sex Date of death Address Phone number	birth to VA MPI. All fields are returned by VA MPI.
Single Sign On Internal (SSOi)	SSOi – Integration with Single Sign-On	User email User full name	HTTPs

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: There is a risk that unauthorized individuals may access the information.

Mitigation: Existing mitigation techniques used to protect privacy from internal sharing and disclosure risks which include training will be utilized. Additionally, we will have consistent monitoring of user access reports and logs. Should any data be lost or compromised, we replicate and create a snapshot of our database on a regular basis for backup purposes.

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.

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***
International Business Machines Corporation IBM IAP/VBAAP Sys	The expected benefit of the interconnection is to expedite the processing of data associated with the VA and IBM	-Name -Social Security Number -Date of Birth -Mailing Address -Zip Code -Phone Number(s) -Fax Number -Email Address -Emergency Contact Information (Name, Phone Number, etc. of a different individual) -Health Insurance Beneficiary Numbers -Previous Medical Records	MEMORANDUM OF UNDERSTANDING AND INTERCONNECTION SECURITY AGREEMENT	TCP trough port 443

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: There is a risk that information could be shared with unauthorized individuals.

Mitigation: Caseflow has one external connection in which IBM implements the following security measures and controls:

- Identification and Authentication - IBM maintains acceptable standards for creating or modifying company user accounts. These standards include provisions for updating, revision, and retirement. All user accounts are handled in accordance with the appropriate security considerations and with regard for the integrity of sensitive data. IBM ensures adherence to appropriate security standards while providing for the best performance in achieving production goals.
- Logical Access Controls - IBM enforces a strict password management policy to protect the integrity of network resources and data and in accordance with VA 6500 and industry guidelines. It is our policy for any instance of a compromised password to be treated as a security incident. We require that all passwords be changed at least once every ninety (90) days. User accounts with system level privileges (granted through group memberships or programs) must have a password unique from all other accounts held by that user.
- Physical and Environmental Security - The IBM IAP environment is hosted on FedRAMP High AWS GovCloud and inherits FedRAMP High Physical and environmental controls for the infrastructure from the Cloud Service Provider. And for the managed Services part, IBM ensures best practices and policies to safeguard company facilities and premises from unauthorized physical access, and to protect the integrity of network resources and data from ensuing threats. IBM abides by the security principle of least privilege. Intrusion detection capabilities are evaluated to secure privileged internal areas. All decisions concerning facility security are made at the executive level, and any modifications must therefore be cleared at the executive level. The Managed Security Services datacenter facility has multiple redundancies built into our system infrastructure.
- Firewall, IDS, and Encryption - IBM IAP environment subscribes to all the firewall, IDS and encryption policies and implementations provided by the AWS GovCloud Cloud Service Provider (CSP) for IAP infrastructure. And at the Managed Security Services

side, IBM maintains multiple policies and procedures which mandate the use of firewalls and encryption. Implementation procedures exist which define the required configurations for security appliances. Encryption is mandated in motion and is addressable at res

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 Caseflow application is used internally and does not collect any information directly from Veterans. It only processes and transfers information in existing systems and procedures. Thus, a notice is not applicable.

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

Data that Veterans provide via other processes (such as by sending mail or interacting with other VA services) may be accessed and stored in Caseflow to support appeals processing and other functions described in the overview. Please review SORN for further information. SORN from the OPRM site **(https://department.va.gov/privacy/)**. **SORN Identifier – (44VA01 / 88 FR 44185- Veterans Appellate Records System-VA"** 2023-14569.pdf (govinfo.gov))

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.

N/A

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.

Caseflow does not collect information directly from individuals but from other systems. Those other systems cover the pertinent notices about declining to provide information and/or any associated penalties in their individual PIAs.

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.

Caseflow does not collect information directly from individuals but from other systems. Those other systems cover the pertinent notices about consent to their uses of the information and/or to exercise individual rights in their individual PIAs.

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: There is a risk that individuals are not notified of their data being collected/used

Mitigation: Caseflow does not collect information directly from individuals but from other systems. Those other systems cover the pertinent notices in their individual PIAs. Caseflow data at rest resides in volumes utilizing EBS encryption. TLS is utilized for the transfer of data.

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.***

Since Caseflow is not available for individuals to have direct access, the individual must submit a FOIA request using the guidance and instructions outlined on the Freedom Of Information Act FOIA (va.gov) or https://www.va.gov/ websites.

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)?

N/A

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?

N/A

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.

Requests can be submitted to the VA using existing procedures (for example, by contacting Regional Office representative or mailing a letter to the VA). Existing procedures will be used to update this information. However, Caseflow will implement improvements to leverages enterprise data, which will more effectively result in corrected data across multiple systems. For example, when a Veteran informs the VA of a new address, by using the Corporate Database, Caseflow can pull this data centrally rather than require an independent update.

Additionally, Caseflow has introduced, where possible, automated error-checking capabilities allowing the user to make corrections in the main system of record which reduce and reconcile error.

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.

Caseflow does not collect any information directly from the public. As such, the system relies on the same notification methods of veteran-facing systems and processes to inform users of how they can correct their information. If the user needs assistance locating details on how to update their information, they can contact the VA using the following website: https://iris.custhelp.com/

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.

Users can request access to his or her records by filing a Privacy Act/Freedom of Information Act Request with the VA. Freedom Of Information Act FOIA (va.gov)

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk of inaccurate information in VBMS and VACOLS, as well as information being entered incorrectly during workflows.

Mitigation: We will monitor user feedback, as well as analyze system data for error rates. Any inaccuracies will be addressed immediately, and fixes can be deployed in an iterative manner. Caseflow will leverage centralized enterprise resources when possible, to ensure that users' requests can be fulfilled across any system using the enterprise resource concurrently. Caseflow will also update these enterprise resources to share corrected information with other systems that leverage these resources. Additionally, individuals can submit a request, as discussed in 7.2, to correct inaccurate or erroneous information.

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?

The Caseflow system will be using Common Security System (CSS) for two-factor user authentication. We will be leveraging the existing CSS process for managing access to roles and functions within the system. This includes requesting new roles and functions as needed to maintain secure control over various features and PII information within each product.

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?

We have three levels of user access (increasing privilege order): typical user, manager, system admin. All of which are granted with a CSEM application request and must complete all levels of approval which include the Information Security Officer (ISO) as final approver. A request for access to Caseflow must come through the Caseflow PM team for initial approval.

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.

Additional security controls within Caseflow have been established for the System Admin user function to ensure only Caseflow team members are granted this elevated production privilege. Server-level access will be managed and granted to developers on a need basis by the Caseflow Information Security Officer (ISO). We will be limiting access to only a small set of trusted developers approved to work with and diagnose production issues. Secure Shell (SSH) access will be logged and monitored. All of these processes have been documented in our Account Management control document and User Access Guidance document.

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.

Caseflow Software Engineers, Research/Designers, Product Managers, Product Support Analysts, Product Trainers and Project Managers, as contractors, will be given access to the system and PII to carry out their daily tasks whether in a support, design, or development/maintenance role as contractually obligated. They will be given System Admin role. All Caseflow contractors are required to sign an NDA and will receive a clearance.

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.

No additional privacy or security training would be offered specific to the Caseflow application. Existing VA privacy, HIPPA and PII trainings are deemed to be sufficient. Access to AWS is provided only after a user completes TMS Course 1357076 Information Security and Privacy Role Based Training for System Administrators. TMS course completion certificate is sent to the Team Lead as proof that the individual can have access to AWS. **8.4 Has Authorization and Accreditation (A&A) been completed for the system?**

8.4a If Yes, provide:

1. *The Security Plan Status:* Yes
2. *The System Security Plan Status Date:* 09/13/2021
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 01/07/2021
5. *The Authorization Termination Date:* 01/07/2024
6. *The Risk Review Completion Date:* N/A
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.***

N/A

Section 9 – Technology Usage

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

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

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

(Refer to question 3.3.1 of the PTA)

Caseflow is hosted within VAEC "VAEC AWS GOVCLOUD HIGH". This FedRAMP approved, FISMA moderate environment provides Infrastructure as a Service (IAAS) capabilities to Caseflow, such as web and database servers for the various applications that comprise Caseflow.

There is no PII information being shared / received with any external organizations as defined in this document. All staff who are authorized to use PII are required to undergo Privacy & HIPAA annual training. Hence, information sharing with **Third Parties is Not Applicable** for Caseflow.

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.*

Caseflow is hosted within Amazon Web Services GovCloud (commercial cloud computing environment). This FedRAMP approved, FISMA moderate environment provides Infrastructure as a Service (IAAS) capabilities to Caseflow, such as web and database servers for the various applications that comprise Caseflow.

There is no PII information being shared / received with any external organizations as defined in this document. All staff who are authorized to use PII are required to undergo Privacy & HIPAA annual training. Hence, information sharing with Third Parties is Not Applicable for Caseflow.

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.

VA owns the ownership rights over PII data for Caseflow. VAEC (AWS GOVCLOUD High) is the hosting environment and provide cloud services such as IaaS, Saas along with a set of common services, security, and connectivity between the cloud environments and the VA network.

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.

Caseflow own logs, audit trials but consumption data used for billing is owned by AWS.

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).

N/A

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.

KARY CHARLEBOIS

Digitally signed by KARY CHARLEBOIS
Date: 2024.01.16 16:41:03 -05'00'

Privacy Officer, Kary Charlebois

Griselda Gallegos 204736

Digitally signed by Griselda Gallegos 204736
Date: 2024.01.18 07:53:53 -06'00'

Information System Security Officer, Griselda Gallegos

JASON RHINEHART

Digitally signed by JASON RHINEHART
Date: 2024.01.18 08:57:02 -05'00'

Information System Owner, Jason Rhinehart

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).

Please review SORN for further information. SORN from the OPRM site https://department.va.gov/privacy/**)**. **SORN Identifier – (44VA01 / 88 FR 44185 - Veterans Appellate Records System-VA"** 2023-14569.pdf (govinfo.gov) **). VA FOIA -** Freedom Of Information Act FOIA (va.gov).

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