Privacy Impact Assessment for the VA IT System called:

Veterans Appeals Control and Locator System (VACOLS)

Veteran's Benefit Administration (VBA)/ Board of Veterans Appeals (BVA)

Date PIA submitted for review:

04/03/2023

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)	Pamela Crockett Williams	Pamela.Crockett-Williams@va.gov	202-382-2341
Information System Owner	Geoffrey Stienblock	Geoffrey.Stienblock@va.gov	(727) 273-6750

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

The Veterans Appeals Control and Locator System (VACOLS) is a shared automated database for tracking and controlling Veterans' appeals of denials of their claims for benefits. Full implementation of Veterans Appeals Control and Locator System (VACOLS) enables Veteran's Benefit Administration (VBA) Regional Offices (RO), the Board of Veterans' Appeals (BVA) staff, Veterans Service Organizations (VSO), the Office of the General Council (OGC), Veterans Administration Liaison staff, Veterans Health Administration (VHA) and National Cemetery Administration (NCA) to report and monitor productivity, quality and pending workloads. The sensitive personal information listed above has been collected from Master Databases. Veterans Service Organizations (VSO), the Office of the General Council (OGC) have read-only access to Veterans Appeals Control and Locator System (VACOLS). The Board of Veterans' Appeals (BVA), Regional Offices (RO), National Cemetery Administration (NCA) and Veterans Health Administration (VHA) employees have written access to Veterans Appeals Control and Locator System (VACOLS) data pertaining to the roles in the appeal process." Veterans Appeals Control and Locator System (VACOLS) is the system of record for appeals within the VA. Veterans Appeals Control and Locator System (VACOLS), provides functionality to the Board of Veterans' Appeals, other departments and stakeholders enabling the processing and tracking of appeals and related processes. The database is used to track appeals of Department of Veterans Affairs Regional Office decisions on benefits available under Title 38 of the United States Code.

Overview

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

1 General Description

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

Veterans Appeals Control and Locator System (VACOLS) is the system of record for appeals within the VA for the Board of Veterans' Appeals

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

VACOLS provides functionality to the Board of Veterans' Appeals, other departments and stakeholders enabling the processing and tracking of appeals and related processes. The database is used to track appeals of Department of Veterans Affairs Regional Office decisions on benefits available under Title 38 of the United States Code.

C. Indicate the ownership or control of the IT system or project.
Department of Veterans Affairs Owned

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
VACOLS contains records for 1.6 million Veterans.

E. A general description of the information in the IT system and the purpose for collecting this information.
The database is used to track appeals of Department of Veterans Affairs Regional Office appeal decisions on benefits available under Title 38 of the United States Code.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
VACOLS shares data with other VA systems Caseflow, eBenefits, and VBA's Customer Relationship Manager (CRM).

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

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.
VACOLS will operate under authority from Title 38 of the United States Code and Title 38 of the Code of Federal Regulations. **Title 38, U.S Code, Sections 501(a) , SORN VACOLS -44VA01/78 FR 66803**

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?
N/A

D. System Changes

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

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

N/A

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Data Element
Appellant Address

PII Mapping of Components (Servers/Database)

Veterans Appeals Control and Locator System (VACOLS) consists of one key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Veterans Appeals Control and Locator System (VACOLS) and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VACOLS – Veterans Appeals Control and Locator System	Yes (shared internally)	Yes (shared internally)	Name, Date of Birth, SSN and Appellant Address	**VACOLS uses SSNs but does not collect them.** They are assigned by (VBA) as claim numbers and until that practice ends, VACOLS will have custody of large quantities of them. SSN are used to identify and track appeals, including identifying/retrieving related data in other systems. SSNs are also found in documents/data that are collected, stored, and retrieved as part of the processes described above. Title 38, U.S Code, Sections 501(a).	Standard two-factor authentication required to access data. Transport Layer Security (TLS) v 1.2 encryption protects the Oracle data in transit and Transparent Data Encryption (TDE) is used to protect the data at rest.

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?

VA Claims, Board of Veterans' Appeals records

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.

Data presented by appellants and their representatives at hearings and in briefs and correspondence; and data furnished by Board of Veterans' Appeals employees.

1.2c If the system creates 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 collected via VA Form 9 – It is an electronic form with VBMS that is managed by Caseflow that collects the data.

- VA Form 9 is filled out by a Veteran seeking an appeal.
- The data is manually entered into the VACOLS system by a VA VACOLS user once the Notice of Disagreement (NOD) has been received

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

VA FORM 9 and VA Form 21-0958 Notice of Disagreement

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.

VACOLS Individual Information Authentication - ORACLE roles have been defined to control update access on a table level. Program logic controls update capability for columns within the database validating both data format integrity and data entry compliance with established business rules and logic & authentication through End user data entry to Oracle database with user logins

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

N/A The information is provided by the individual. The only check for accuracy would be the individual reviewing the content of the information provided. The system does not have any technical means for checking for data 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

38 U.S.C. 7101(a), 7104, Composition of the Board of Veterans' Appeals;
5 U.S.C. 552, The Freedom of Information Act.
Title 38, U.S Code, Sections 501(a).
SORN VACOLS -44VA01/78 FR 66803

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The VACOLS team system maintains Personally Identifiable Information (PII) and Personal Health Information (PHI) in order to carry out the mission of processing appeals for VA benefits. If this information were to be compromised or released to inappropriate parties or the public there could be significant financial, personal, and/or emotional harm to the individuals whose information is contained within the VACOLS system

Mitigation: The Department of Veterans Affairs (VA) VACOLS team is careful to only collect the information necessary to carry out the mission of processing appeals for veterans' benefits. By only collecting the minimum PII and PHI needed to process appeals for veterans the risk to veterans is also minimized in the event of a data breach.
All employees, contractors, volunteers, etc, who have access to the information in VACOLS are trained by the Board in the appropriate use of the information and also complete the required annual Privacy and Information Security Training and sign the Rules of Behavior annually. All are aware of the penalties of misusing information to which they have permissive access"

Section 2. Uses of the Information

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

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

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

All information contained within the VACOLS system pertaining to appeals is used for the Veterans Appeals process.

- ☒ Name – Used to identify appellant and address correspondence.
- ☒ Social Security Number - Used to identify an appellant.
- ☒ Date of Birth – used to calculate Advance on Docket (AOD) status for advanced age.
- ☒ Personal Mailing Address – used for correspondence with appellant.
- ☒ Personal Phone Number(s) – used for correspondence with appellant.
- ☒ Personal Fax Number – used for correspondence with appellant.
- ☒ Personal Email – used for correspondence with appellant.
- ☒ Appellant Mailing address – used for correspondence with appellant when appellant is different from veteran.

All information for VA employees contained within the VACOLS system is used to determine user access levels to the VACOLS application for the employee's assigned business process.

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.

All data contained within the VACOLS system is analyzed and used only within the VACOLS system. No external program is used to analyze the data

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

N/A

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 VACOLS system can only be accessed by VA users via standard VA two-factor authentication.

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

Transparent Data Encryption (TDE) is used to protect the data at rest in Oracle Database.

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

Transport Layer Security (TLS) v 1.2 encryption protects the Oracle data in transit and Transparent Data Encryption (TDE) is used to protect the data 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?

All VA employees and contractors are required to go through privacy, information security and VA Rules of Behavior (ROB) training. This training ensures that the end users of the VACOLS know

how to properly handle PII. Beyond the training the system is designed to secure the data to ensure that users must be granted access to the system in order to view, modify, add or remove data.

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

All training is documented and tracked through VA TMS (https://www.tms.va.gov)

2.4c Does access require manager approval?

Yes, a Service NOW work ticket has to be submitted by the users Manager in order to access VACOLS.

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

It is assumed that all VACOLS users will be viewing PII to that extent access to database is recorded for individual users. Access to VACOLS is terminated after 60 days of inactivity or when a user leaves VA or is reassigned to a job not requiring VACOLS access.

N/A *2.4e Who is responsible for assuring safeguards for the PII?*

Any Veteran Affairs employee who is an authorized Veterans Appeals Control and Locator System (VACOLS) system user or administrator has the responsibility for assuring safeguard for PII.

Section 3. Retention of Information

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

3.1 What information is retained?

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

***Name-** First and last name of the individual. Used to identify Patient in other forms of communication.*
***Date of birth**- Individual's date of birth*
***SSN**- Social security number of the individual*
***Email**- Email of the individual*
***Appellant address**- Used as an identifier and identify patients address*

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.*

Records are retained in accordance with records retention standards approved by the Archivist of the United States, the National Archives and Records Administration, and published in Agency Records Control Schedules. The retention schedules are documented in the SORN. **VACOLS covers Appeals data information in database almost dating back the last 27 years** Records in this system, in VACOLS, and those collected prior to VACOLS' use as a repository are retained indefinitely as Category B Vital Records unless otherwise specifically noted. Under the Vital Records Schedule, electronic back-up tapes are destroyed by erasure upon receipt of the next quarterly tape set. Recordings of hearings will be made as described in Rule 714, 38 CFR 20.714, and transcriptions of recordings of hearings will be attached electronically in VACOLS. Electronic recordings of hearings will be retained for at least one year from the date of the hearing, giving the hearing subject the opportunity to challenge the accuracy of the transcript.

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:
https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-veterans-affairs/rg-0015/n1-015-90-001_sf115.pdf

Medical Administration Service Records – N1-015-87-004
Veterans Medical Records Folder – N1-015-90-005
Perpetual Medical Files - N1-015-91-007
Electronic Patient Medical Record - N1-015-02-003

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.

VACOLS appeals data currently in the database dates back to 1993. VACOLS currently covers 27 years of appeals data in database. Hearings before the Board are digitally recorded and stored indefinitely. *Where a facility must use audio tape to record hearings, the recording is maintained for one year after which period it is destroyed*. A transcript is made for each hearing held and is electronically attached to the record in VACOLS. Digital recordings of hearings are maintained on a back-up server. Under the Vital Records Schedule, electronic back-up tapes are updated quarterly. A back-up tape is transferred weekly to the Board's contractor for quick access back-up tape storage.
"Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. file:///C:/Users/VACOOkereB/Documents/Directive_6500_24_Feb_2021%20(2).pdf"

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.

All VACOLS documentation and training materials use fictitious appellant information for screen shots and sample reports. No PII is used in training materials or user documentation. All requests for VACOLS data for research purposes from VA, other Government Agencies or the private sector are redacted and all PII data fields are removed from research data requests.

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 always a risk that information could be retained for longer than necessary.

Mitigation: ORACLE roles have been defined to control update access on a table level for unauthorized access. User logins for Oracle database access. Access to VACOLS is strictly limited to reflect the need for the different records in the system. Where a Veterans Service Organization office is located in a VA facility and has access to VACOLS through the Wide Area Network, that access is strictly limited to viewing records of current clients of the organization. No personal identifiers are used in statistical and management reports, and personal identifiers are removed from all archived Board of Veterans' Appeals decisions and other records in this system before VA makes them available to the public.

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***
eBenefits.va.gov	To provide veterans with the status and or resolution of their appeal.	SSN, Name & Address	Weblogic direct connect
CRM (Customer Relationship Mgmt)	To provide veterans with the status and or resolution of their appeal.	SSN, Name & Address	Weblogic direct connect
Caseflow Assessing	For tracking appeals status	SSN,Name and Address	SSL over TCP database connections

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: Any appeals data that is being shared internally has potential risk associated within the Department due to the previously defined PII contained in the VACOLS database.
Mitigation: VA employees, including employees of the Board of Veterans' Appeals and its contractors, all of whom have a need to know the contents of the system of records in order to perform their duties. Access to VACOLS is strictly limited to reflect the need individual employees have for the different records in the system sharing internally. No personal identifiers are used in statistical and management reports.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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>
Mitigation: <Not Applicable>

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 VACOLS has an SORN which is currently being updated posted on the Federal Register((https://www.oprm.va.gov/privacy/systems_of_records.aspx).
Veterans Appeals Control and Locator System (VACOLS) – Veterans Appellate Records System-VA." Sorn Number - 44VA01/78 FR 66803). A Privacy Act Statement is provided on any forms that collect information from individuals. PRIVACY ACT STATEMENT: Our authority for asking for the information you give to us when you fill out this form is 38 U.S.C. 7105(d)(3), a Federal statute that sets out the requirement for you to file a formal appeal to complete your appeal on a VA benefits determination. You use this form to present your appeal to the Board of Veterans' Appeals (Board). It is used by VA in processing your appeal and it is used by the Board in deciding your appeal. Providing this information to VA is voluntary, but if you fail to furnish this information VA will close your appeal and you may lose your right to appeal the benefit determinations you told us you disagreed with. The Privacy Act of 1974 (5 U.S.C. 552a) and VA's confidentiality statute (38 U.S.C. 5701), as implemented by 38 C.F.R. 1.526(a) and 1.576(b), require individuals to provide written consent before documents or information can be disclosed to third parties not allowed to receive records or information under any other provision of law. However, the law permits VA to disclose the information you include on this form to people outside of VA in some circumstances. Information about that is given in notices about VA's "systems of records" that are periodically published in the Federal Register as required by the Privacy Act of 1974. Examples of situations in which the information included in this form might be released to individuals outside of VA include release to the United States Court of Appeals for Veterans Claims, if you later appeal the Board's decision in your case to that court; disclosure to a medical expert outside of VA, should VA exercise its statutory authority under 38 U.S.C. 5109 or 7109, to ask for an expert medical opinion to help decide your case; disclosure to law enforcement personnel and security guards in order to alert them to the presence of a dangerous person; disclosure to law enforcement agencies should the information indicate that there has been a violation of law; disclosure to a congressional office in order to answer an inquiry from the congressional office made at your request; and disclosure to Federal government personnel who have the duty of inspecting VA's records to make sure that they are being properly maintained

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

VACOLS has an SORN which is currently being updated posted on the Federal Register (https://www.oprm.va.gov/privacy/systems_of_records.aspx). Veterans Appeals Control and Locator System (VACOLS) – Veterans Appellate Records System-VA." Sorn Number - 44VA01/78 FR 66803).

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

Notice states the requirement of what the form is being used for, and it states that the form is voluntary.

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.

Individuals do have the opportunity and right to decline to provide information. In the event that any information is not provided, the individual's appeal might not be able to be processed and the appeal could be denied.

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.

The individual must give consent in order for their information to be used as part of an appeal .
VACOLS does not collect information directly from individuals but from other systems. Those other systems cover the pertinent notices about consent to their particular uses of the information and/or to exercise individual rights in their individual PIAs.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>
Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: There is a risk that individuals are not notified of their data being collected/used. The individual providing information to be used for an appeal is provided with the Privacy Act Notice and the SORN **VACOLS -44VA01/78 FR 66803** is available for review.

Mitigation: VACOLS does not collect information directly from individuals but from other systems. Those other systems cover the pertinent notices in their individual PIAs. All of VACOLS data is protected by Transport Layer Security (TLS) v 1.2 encryption, which protects the Oracle data in transit and Transparent Data Encryption (TDE) which is used to protect the data at rest.

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.***

Access to and use of national administrative database are limited to those people whose official duties require such access, and the VA has established security procedures to ensure that access is appropriately limited. Information security officers and system data stewards review and authorize data access requests. VA provides information security training via the Talent Management System (TMS) to all staff and instructs staff on the responsibility each person has for safeguarding data confidentially.

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).

Members of the public are not allowed to access the VACOLS system directly Individuals seeking information regarding access to information contained in this system of records may write or call the Board of Veterans' Appeals Freedom of Information Act Officer, whose address and telephone number are as follows: Freedom of Information Act Officer (01C1), Board of Veterans' Appeals, 810 Vermont Avenue NW., Washington, DC 20420 FOIA. Contact No FOIA officer – 202-322-3652

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.

Since VACOLS is not available for individuals to have direct access, the individual must submit a FOIA request using the guidance and instructions outlined on the **http://www.va.gov/foia/**or **http://www.vets.gov** websites

"The Freedom of Information Act (FOIA), 5 U.S.C § 552 and the Privacy Act of 1974, 5 U.S.C § 552a provide individuals access to their information"

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 VA procedures that conform to the Privacy Act. For example, a veteran can contact a Regional Office representative, or the veteran can mail a letter to the VA requesting the correction. Once the information is received by the VA the update is performed manually by VA employees in Regional Offices that manage the VACOLS case data.

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.

Individuals are not notified if there is missing or inaccurate information in their record. An individual who wishes to determine whether a record is being maintained under his or her name in the VACOLS system or wishes to determine the contents of their records show follow the instruction to use the website.
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/. Alternatively, Individuals seeking

information regarding access to information contained in this system of records may write or call the Board of Veterans' Appeals Freedom of Information Act Officer, whose address and telephone number are as follows: Freedom of Information Act Officer (01C1), Board of Veterans' Appeals, 810 Vermont Avenue NW., Washington, DC 20420 VACO FOIA Officer 202-322-3652

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. (*http://www.va.gov/foia/)*

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: The individual could accidentally provide incorrect information in their correspondence.

Mitigation: Individuals provide information directly to VA staff or contractors. Any validation performed would merely be the individual personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence while indicating to the VA that new information supersedes the previous data

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.

Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring are performed through the use of the Talent Management System (TMS).
The VACOLS will be using Two Factor authentication to allow users internal to VA access to the system using PIV/PIN.

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?

VACOLS does not share any information externally. Therefore, other agencies will not have access to VACOLS.

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.

Server level access is granted to developers on an as needed basis by the VACOLS Information Security Officer (ISO). The VACOLS ISO has granted server access to a small set of trusted developers approved to work with and diagnose production issues. Remote Desktop Protocol (RDP) and Secure Shell (SSH) access is logged and monitors.

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

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

Yes, there are contract personnel who maintain the software and system documentation. These contractors are not primary users of the VACOLS. Contactors who provide support to the system are required to complete annual training covering VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Manage System (TMS). Background investigation and adjudication is completed on contract personnel serving in this role. Contractors will be given access to commit code to the application and complete their contractual obligations. Contracts are reviewed quarterly by the Contract Officer Representative.

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 VA employees and contractors are required to go through the following VA TMS training course annually

- VA Privacy & HIPAA Training annually.
- Information Security Awareness and Rules of Behavior annually

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* March 15th, 2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* February 13th, 2023
5. *The Authorization Termination Date:* May 6th, 2023
6. *The Risk Review Completion Date:* January 24th, 2023
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.***

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)*

Not applicable. VACOLS does not operate in a Cloud environment.

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.*

Not applicable. VACOLS does not operate in a Cloud environment.

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.

Not applicable. VACOLS does not operate in a Cloud environment.

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.

Not applicable. VACOLS does not operate in a Cloud environment.

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).

Not applicable. VACOLS does not operate in a Cloud environment.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

KARY CHARLEBOIS

Digitally signed by KARY CHARLEBOIS
Date: 2023.04.12 18:41:06 -04'00'

Privacy Officer, Kary Charlebois

Crockett-Williams, Pamela

Digitally signed by Crockett-Williams, Pamela
Date: 2023.04.18 08:55:39 -04'00'

Information Systems Security Officer, Pamela Crockett Williams

Geoffrey A. Stienblock 1665653

Digitally signed by Geoffrey A. Stienblock 1665653
Date: 2023.04.13 13:42:32 -04'00'

Information Systems Owner, Geoffrey Stienblock

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).

Sorn- (https://www.oprm.va.gov/privacy/systems_of_records.aspx).
Veterans Appeals Control and Locator System (VACOLS) – Veterans Appellate Records System-VA." Sorn Number - 44VA01/78 FR 66803).

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices