



Privacy Impact Assessment for the VA IT System called:

Common Functional APIs (CFAPI)

Veterans Benefits Administration

Office of Information Technology

eMASS ID # 2048

Date PIA submitted for review:

08/23/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Sammy L. Thomas	Sammy.thomas@va.gov	404-929-5797
Information System Security Officer (ISSO)	Joseph Facciolli	Joseph.Facciolli@va.gov	215-842-2000
Information System Owner	Christina Lawyer	Christina.lawyer@va.gov	518-210-0581

Abstract

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

The Common Functional APIs (CFAPI) provides applications residing within the Benefits & Integration Platform (BIP) a programmatic interface for Create Read Update and Delete (CRUD) operations for Veteran profile, notes and claims data. CFAPI is comprised of Notes API Veteran API and Claim Automation processor. The Notes Application Programming Interface (API) is a service that supports accessing Veteran and Claim Development Note data as is consistent with its use inside of the claim processing domain. The Veteran Application Programming Interface (API) is a service that supports accessing Veteran data as is consistent with its use inside of the claim processing domain. The Claim Automation Processor is a background process that listens for file change events from the Veteran Enterprise File Storage Systems (VEFS) which includes eFolder. The Claims Automation Processor will monitor new files and create new claims as needed.

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?

The Common Functional APIs (CFAPI) is under the authority, of the Office of Information Technology (OIT).

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

Manage Claimant Record is the ability to verify service and record, create a new one, or reconcile duplicate or distinct records in support of claims establishment.

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

CFAPI is owned and controlled by the controlled by the Office of Information Technology (OIT).

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?

All Veterans and dependents of Veterans will have information stored or processed by this system. The expected number of Veterans and/or dependents is around 100 thousand to possible over millions.

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

Information is collected and processed for Veterans and dependents including First & Last Name, Address, Date of Birth, Date of Death (if applicable), Social Security Number, Phone, Gender, Email, Integration control number, Military History to support C&P/VBMS applications that need to access this data to process claims.

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

CFAPI shares information with the Notes API which is a service that is intended to support accessing Veteran and Claim Development Note data as is consistent with its use inside of the claim processing domain. CFAPI shares information with the IDB (Interactive Development Banner) Admin Application Programming interface (API) which is the API between IDA (Interactive Development Architecture) Admin UI (User Interface) and Rule Execution Flow. CFAPI shares information with the STR (Service Treatment Request) Assist API which the STR Assist application allows users to submit STR requests to various repositories to obtain the appropriate documentation necessary to process related claims.

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?*

CFAPI resides on the BIP Platform only and therefore has no issues with synchronization.

3. *Legal Authority and SORN*

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

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104--- 231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- Privacy Act of 1974; U.S Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 & Title38, US Code section 7301 (a) and Executive Order 9397
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) •
- State Privacy Laws
- The legal authority is 38 U.S.C 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

The System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (July 19, 2012).

This SORN can be found online at <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

- 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?*

No amendments or revision to SORN is required.
Yes, the SORN does cover cloud usage.

The System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 - This SORN can be found online at <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048 5 U.S.C. § 552a, Privacy Act of 1974, As Amended IRS memo FD698-FED-AWS GovCloud-L-031020

4. System Changes

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

Completion of this PIA will not result in changes to existing business processes.

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

Completion of the PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Other PII/PHI data elements: Date of Death (DoD)

PII Mapping of Components (Servers/Database)

CFAPI consists of **one** 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 **CFAPI** 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

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

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
Corporate Database (CorpDB)	Yes	Yes	<ul style="list-style-type: none"> • First Name • Last Name • Address • Date of Birth (DoB) • Date of Death (DoD) • Social Security Number • SSN • Phone number • Gender • Email • • Integration control number (ICN) • Military History 	Manage Data Repository is the control of a large data storage structure that collects, manages, and stores datasets for analysis, sharing, and reporting.	RLS application team verifies that DB is up to date with versioning security standards.

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?

Listed below are the systems which are the source of data processed by CFAPI.

- Notes API
- IDB Admin Application Programming interface (API)
- Participant API
- Power of Attorney API

- STR Assist API

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.

CFAPI provides applications residing within the Benefits Integration Platform (BIP) a programmatic interface for Create Read Update and Delete (CRUD) operations for Veteran profile, notes and claims data. CFAPI is a generic, abstract namespace used to house API components that may interact with one or more other functional components in BIP tenants but that do not necessarily interact functionally with each other.

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

CFAPI uses the listed application above to access this data to provide BIP tenants with access for purposes of creating, reading and updating this information as it relates to processing and handling of claims.

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 electronically received and updated data via HTTPS /SOAP and Request/Response are Secured by SAML and HTTPS.

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

Information is not collected on a form.

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.

Accuracy checking of this information is currently happening through the Master Person Index (MPI) service as they can correlate information from multiple separate systems (Corp/IBS/VAPProfile/VADIR/etc). This is done on an ad hoc basis and during MPI queries they will return information denoting if there is conflicting information or catastrophic edits.

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?

No, a commercial aggregator is not used MPI is a VA service.

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

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104--- 231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- Privacy Act of 1974; U.S Code title 5 USC section 301 title 38 section 1705, 1717, 2306-2308 & Title38, US Code section 7301 (a) and Executive Order 9397
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) •
- State Privacy Laws
- The legal authority is 38 U.S.C 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

The System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (July 19, 2012). This SORN can be found online at <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: Source data from Notes API, IDB Admin Application Programming interface (API), Participant API, Power of Attorney API, or STR Assist API could be incorrect and could be passed on to calling application.

Mitigation: System controls validate data inputs, and their many business rules are executed against the data prior to any decisions. Additionally, there is a full audit trail of system actions and decisions. All data is sourced from trusted VA systems that also have data integrity and privacy controls.

Privacy Risk: System being compromised, and data stolen.

Mitigation: The system uses strong security controls. The Department of Veterans Affairs applies consistent security guidance to centralize and standardize account management, network access control, database security, vulnerability scanning and remediation.

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
First Name	Used to identify Veteran	Not used
Last Name	Used to identify Veteran	Not used
Address	Used for correspondence with Veteran	Not used
Date of Birth (DoB)	Used to identify the Veteran	Not used
Date of Death (DoD)	Used to identify and for claims	Not used
Social Security Number SSN	Used to verify the identity of the Veteran	Not used
Phone	Used for contacting Veteran	Not used
Gender	Used for verifying identity	Not used
Email	Used for contacting Veteran	Not used
Integration control number (ICN)	Used to verify identity of the Veteran	Not used
Military History	Used to determine eligibility	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?

This system does not perform this action.

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.

This system does not perform this action.

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?

All data is encrypted during transit using SSL. Data at rest is only accessible by system administrators and privileged users that are granted access through a standard approval process. Data at rest is obfuscated.

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

All requests require SSL encryption and a JWT.

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

Data is stored in a secure enclave within AWS. Access to information is protected by industry standard authentication and authorization protocols. Data is encrypted both in transit and at rest via SSL/TLS.

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?

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training, which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the ROB, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

Yes

2.4c Does access require manager approval?

Yes

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

Yes

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

The Platform Accelerator teams control the security safeguards that are in all applications that use the BIP framework.

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*

- First Name
- Last Name
- Address
- Date of Birth DoB
- Date of Death DoD
- Social Security Number SSN
- Phone
- Gender
- Email
- Integration control number (ICN)
- Military History

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.

Data is maintained indefinitely per VA data retention policies.

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?

VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII as authorized by NARA

https://www.benefits.va.gov/WARMS/docs/regs/RCS_1.doc

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.

The data is maintained indefinitely. No data elimination is required at this time.

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.

Test data is used during the design and development process. Access to PII in the production environment is controlled to specific VA systems.

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: Incorrect data could be sent to CFAPI from other APIs on the BIP framework.

Mitigation: System controls validate data inputs and there many business rules are executed against the data prior to any decisions. Additionally, there is a full audit trail of system actions and decision. All data is sourced from trusted VA systems that also have data integrity and privacy controls.

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
IDB (Interactive Development Banner) Admin Application Programming interface (API)	It is the API between IDA Admin UI and Rule Execution Flow.	<ul style="list-style-type: none"> • First Name • Last Name • Address • Date of Birth DoB • Date of Death DoD • Social Security Number SSN • Phone • Gender • Email • Integration control number (ICN) • Military History 	Receives and updates data via HTTPS /SOAP Request/Response. Secured by SAML and HTTP
STR(Service Treatment Request) Assist API	The STR Assist application allows users to submit STR requests to various repositories to obtain the appropriate documentation necessary to process related claims.	<ul style="list-style-type: none"> • First Name • Last Name • Address • Date of Birth DoB • Date of Death DoD • Social Security Number SSN • Phone • Gender • Email • Integration control number (ICN) 	Receives and updates data via HTTPS /SOAP Request/Response. Secured by SAML and HTTP

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
		<ul style="list-style-type: none"> • Military History 	
Notes API	The Notes API is a service that is intended to support accessing Veteran and Claim Development Note data as is consistent with its use inside of the claim processing domain.	<ul style="list-style-type: none"> • First Name • Last Name • Address • Date of Birth DoB • Date of Death DoD • Social Security Number SSN • Phone • Gender • Email • Integration control number (ICN) • Military History 	Receives and updates data via HTTPS /SOAP Request/Response. Secured by SAML and HTTP
Participant API	Participant API facilitates the retrieval of any person in the VA system with a participant ID. Participant API currently utilizes data sourced from Benefits Integration Services (BIS) and/or MPI depending on how the Participant API application is configured.	<ul style="list-style-type: none"> • First Name • Last Name • Address • Date of Birth DoB • Date of Death DoD • Social Security Number SSN • Phone • Gender • Email • Integration control number (ICN) • Military History 	Receives and updates data via HTTPS /SOAP Request/Response. Secured by SAML and HTTP
Power of Attorney API	Power of Attorney API will retrieve a list of individuals with Power of Attorney for an individual with a participant ID along with a corresponding address from BIS.	<ul style="list-style-type: none"> • First Name • Last Name • Address • Date of Birth DoB • Date of Death DoD • Social Security Number SSN • Phone • Gender • Email • Integration control number (ICN) • Military History 	Receives and updates data via HTTPS /SOAP Request/Response. Secured by SAML and HTTP

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: The privacy risk associated with accessing and maintaining PII is that this data may be disclosed to individuals who do not require access, which would increase the risk of the information being misused.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized by the system. Further, SPI is always encrypted while in transit.

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

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
None				

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: None, as there is no sharing of information outside of VA with external parties.

Mitigation: None, as there is no sharing of information outside of VA with external parties.

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.

VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service Members, Reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran's benefits administered by VA. See the statutory provisions cited in "Authority for maintenance of the system. This notice is provided by the SORN for better understanding to the reader. The System of Record Notices (SORN) listed in the Federal Register:
58VA21/22/28: Compensation, Pension, Education, and Rehabilitation Records- VA,
<https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

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

The System of Record Notices (SORN) listed in the Federal Register:
58VA21/22/28: Compensation, Pension, Education, and Rehabilitation Records- VA,
<https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

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.

The Department of Veterans Affairs provides public notice that the system exists in two ways:

1. The System of Record Notices (SORN) listed in the Federal Register:
58VA21/22/28: Compensation, Pension, Education, and Rehabilitation Records- VA, <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

2. This Privacy Impact Assessment (PIA) also serves as notice of the EDW. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs “after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.”

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 have the right to decline providing information to VA personnel. However, failure to provide information may result in denial of access to health care benefits. Veterans and their family or guardian (spouse, children, parents, grandparents, etc.) may not decline or request their information not be included as part to determine eligibility and entitlement for VA compensation and pension benefits and also designate a guardian to manage the VA compensation and pension benefits.

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.

While individuals may have the ability to consent to various uses of their information at the VA, they are not required to consent to the use of their information as part to determine eligibility and entitlement for VA compensation and pension benefits. The Privacy Act and VA policy require that PII information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

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: Members of the public may not know that CFAPI exists within VA.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as identified in Section 6.1, including the System of Record Notice and Privacy Act statement.

Section 7. Access, Redress, and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at <http://www.foia.va.gov/> to obtain information about FOIA points of contact and information about agency FOIA processes.

Veterans and authorized parties have a statutory right to request a copy of or an amendment to a record in VA's possession at any time under the Freedom of Information Act (FOIA) and the Privacy Act (PA). VA has a decentralized system for fulfilling FOIA and PA requests. The type of information or records an individual is seeking will determine the location to which a request should be submitted.

FOIA Request

To file you must "[Register](#)" with PAL.

Submit a proper request.

Access the VA FOIA Reading Room for previously released documents.

Request status updates on your submitted request.

Learn about processing fees, fee waivers, and requester categories.

Privacy Act Request

There are **two options** to submit a Privacy Act request, either:

- Privacy Act requests can be made by completing the **entire** [VA Form 20-10206, Freedom of Information Act or Privacy Act](#)

- Send a written request to the Centralized Support Division, including the individual's Social Security number or C-File number may aid in the identification of records.

Centralized Support Division mailing address and email:

Department of Veterans Affairs
Evidence Intake Center
P.O. Box 4444
Janesville, WI 53547-4444
FOIA.vbarmc@va.gov.

Note: When sending a request by email, the signed request **must** be included as an email attachment and include the wet signature.

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)?

This system is not exempt.

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?

The procedure is covered under the System of Record Notices (SORN) as well as provide information listed in question 7.1a.

58VA21/22/28: Compensation, Pension, Education, and Rehabilitation Records- VA,
<https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

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.

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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 or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the records are located. Requests should contain the full name, address and telephone number of the individual making the inquiry. (Per 58VA21/22/28 SORN)

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 ensure data accuracy.***

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans and other beneficiaries may contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information.

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: Source data from Notes API, IDB Admin Application Programming interface (API), Participant API, Power of Attorney API, or STR Assist API could be incorrect and could be passed on to calling application.

Mitigation: CFAPI does not maintain data nor provide individual access to records. Overall system controls validate data inputs and their many business rules are executed against the data prior to any decisions. Additionally, there is a full audit trail of system actions and decisions. All data is sourced from trusted VA systems that also have data integrity and privacy controls.

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?

Access to PII is granted by the consuming application of CFAPI and is determined based on the user's roles as defined in the Policy Decision Document (PDD) and other security information including security level & station of jurisdiction (SOJ) using the Common Security Users Management (CSUM).

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?

Access to PII is granted by the consuming application of CFAPI and is determined based on the user's roles as defined in the Policy Decision Document (PDD) and other security information including security level & station of jurisdiction (SOJ) using the Common Security Users Management (CSUM). Only approved users from other VA systems/projects can be granted access by VA CSUM. The ISO, ISSO, and Program Managers from the various systems documented establish the criteria for which PII is shared.

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.

The ISO, ISSO, and Program Manager of the system can approve access to the read, read-write, admin roles through VA CSUM.

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.

CFAPI is an application interface thus any access is gained programmatically by the calling application on the BIP platform. Contractors will have access to design and maintenance of applications that utilize the CFAPI. The contractors are under contract for this work and under NDA as well as other contract specific non-disclosure agreements.

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's Talent Management System 2.0 (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 2.0 system.

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: 02/15/2024*
- 3. The Authorization Status: Approved*
- 4. The Authorization Date: 11/20/2023*
- 5. The Authorization Termination Date: 11/20/2026*
- 6. The Risk Review Completion Date: 06/06/2024*
- 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 (ITMAaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1. (Refer to question 3.3.1 of the PTA)

Yes, the system is hosted on BIP which is hosted in the VA Enterprise Cloud (VAEC).

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.

No

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

No

9.4 NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

No

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as “Bots” or Artificial Intelligence (AI).

No

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.

Privacy Officer, Sammy L. Thomas

Information System Security Officer, Joseph Faccioli

Information System Owner, Christina Lawyer

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).

58VA21/22/28: Compensation, Pension, Education, and Rehabilitation Records- VA,
<https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>

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 1605.4: Notice of Privacy Practices](#)