Privacy Impact Assessment for the VA IT System called:

Document Generator

Veteran Benefit Administration (VBA)

Office of Information Technology (OIT)

Date PIA submitted for review:

9/7/23

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Jean-Claude Wicks*	*jean-claude.wicks@va.gov*	*(202) 502- 0084*
Information System Security Officer	*Joseph Facciolli*	Joseph.Facciolli@va.gov	(215) 983- 5299
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?" and will be published online to accompany the PIA link.

Benefits Integration Platform (BIP) provides a container-based application platform in VA Enterprise Cloud (VAEC) AWS in which VA benefits, appeals, and memorial (BAM) applications can be hosted. In addition, BIP, as a General Support Systems (GSS), will further support VA minor application tenants by constraining the controls necessary for applications hosted on the platform.

The Document Generator (DocGen) provides functionality to generate documents and manage limited changes to content templates and attachments used by the service. A plug-in architecture is used whereby different development teams will be able to create a set of templates and related items that can be used to generate documents meeting a specific business need. These plugins can be developed, maintained and deployed independently. As such, the DocGen Service will end up consuming and storing information, but will generally be unaware of the nature of the contents as the specifics are dictated by the plugins. Consequently, the assumption is that any and all types of data may be touched by the system and controls are designed accordingly.

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.

Document Generator – Office of Information Technology

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

The Document Generation Service and Management Tool (DocGen) provides functionality around document generation. It is managed by the Office of Benefits, Appeals and Memorials (BAM). The functionality falls into two primary areas: • Document Generation - The ability to generate a wide variety of documents, via a plugin model. • USI Metadata - The ability to store metadata about a document and stamp the document with an identifier. This identifier can later be read by automated systems and the metadata can be retrieved. The nature and content of the metadata is determined by the needs of the client systems and is controlled by the individual plugins. Note: USI Metadata consists of a set of name/value pairs. The nature of the contents is solely determined by the client systems and is managed by the plugins. The DocGen Service does not do any processing on this data beyond storing it and providing it for retrieval. Additionally, it should be noted that one of the primary goals of the USI is to eliminate the need to place PII or SPI on generated documents. Instead, a non-identifying code is placed on the document (via a QR or Bar code) and the PII or SPI is stored as metadata. Then, should additional processing need to take place at a later date – for example when a letter or form is returned to the VA, the USI is scanned and the PII/SPI is retrieved, along with whatever other data is needed to support the process. The Service and Tool will be

hosted on the Benefits Integration Platform (BIP), which is an OpenShift Container Platform that is hosted in VAEC (AWS).

DocGen Automated Document Generator (ADG) Service is a document intake system for handling the ingestion and processing of files, developed to replace the legacy Batch File Interface (BFI) application as a part of the broader efforts to decommission Virtual VA (VVA). ADG – User Interface (ADG-UI) is a multi-faceted admin-facing interface that will allow for the maintaining and updating of the ADG system via a convenient web application. ADG itself does not handle any of the specific documents and is instead an orchestration system that oversees the flow of documents form the batches into the processing system. ADG-UI will provide metrics for processed batches, allow targeted retrying or manual filling of any failed or otherwise unsuccessful batch files, and allow for the creation and updating of pre-defined batch file routines.

The DocGen-plugin for Printing of Unidentified Records (PURDG) only stores DocGen-plugin profile information in the PUR database. The DocGen plugin will contain a template of the instruction letter. Information will be passed to the DocGen-plugin to populate the instruction letter and a pdf document will be generated. This document will be stored in the Claim Evidence S3 bucket. The generated instruction letter will be packaged with the scanned mail items and mailed back to the sender.

C. Indicate the ownership or control of the IT system or project.

VA owned and VA Operated

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.

The consumers of this service are expected to participate with other authoritative systems in the VA context. The expected number of users whose information is stored in the system can between 50001 – 75000.

E. A general description of the information in the IT system and the purpose for collecting this information.

Document Generator places information onto a generated document or stored in relation to a USI for use in further downstream processing.

Information in the system typically includes:

- Name
- Sender name
- Social security number
- File number
- Date of birth
- Mother's maiden name
- Personal mailing address
- Sender mailing address
- Personal phone number

- Personal fax number
- Personal email address
- Emergency contact name
- Emergency contact phone number
- Financial account information
- Health insurance beneficiary numbers
- Account numbers
- Certificate/license number
- Vehicle license plate number
- IP address
- Current medications
- Previous medical records
- Race/ethnicity
- Tax identification number
- Medical record number
- Document types of correspondence received

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

The Service and associated Tool are hosted on BIP. Benefits Integration Platform (BIP) provides a container-based application platform in VAEC AWS in which VA benefits, appeals, and memorial (BAM) applications can be hosted. The platform leverages Kubernetes clusters for container management and orchestration, which allows teams to develop, scale, and deliver modern, secure, and properly segmented (from a storage, network, and compute perspective) applications in a multi-tenant environment. The AWS Virtual Private Clouds (VPCs) within BIP are sequentially peered to allow connectivity between VPCs, which supports the promotion of container images from lower VPCs to higher VPCs. The peering is essential for DevOps and Agile methodologies and is locked down to only allow container images to be mirrored between registries in each VPC. BIP also leverages a suite of TRM approved COTS tools (e.g. Jenkins, SonarQube, Vault, Nexus, Consul) to help development teams deliver quickly and effectively. In addition, BIP, as a General Support Systems (GSS), will further support VA minor application tenants by constraining the controls necessary for applications hosted on the platform.

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.

BIP is operated in a single instance of the VA Enterprise Cloud (VAEC) AWS GovCloud, deployed across three Availability Zones.

The systems are minor applications under the BIP Assessing system/project. It falls under the BIP Assessing Authority to Operate (ATO). All controls and hosting agreements with AWS are inherited from AWS VAEC GovCloud and BIP. BIP leverages the VAEC Cloud Service Provider (CSP) AWS GovCloud, which is FEDRAMP approved. Per the approval of the

Deputy Assistant Secretary, Enterprise Program Management Office (EPMO) [the VA Authorizing Official (AO)], BIP has an ATO for one calendar year, effective February 13, 2019. VA Business Stakeholders of the BIP minor applications have ownership rights over data.

The system processes PII related to veterans and dependents. PII data may end up being stored by the system, either as USI Metadata or embedded in generated PDFs. This will be dictated by the needs of each plugin.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

Document Generator operates under the following legal authority:

- Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
- Information from the SORN: 38 U.S.501(a)C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E
- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,
- VA Directive and Handbook 6502, Privacy Program

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The system will not require amendment or revision.

D. System Changes

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

The completion of this PIA is not expected to result in business process changes.

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

The completion of this PIA is not expected to 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.

The Document Generator provides functionality around Document generation and seeks to provide simple and concise mechanisms to create these documents manage changes to content templates. The functionality falls within two primary areas:

- Document Generation - The ability to generate a wide variety of documents, via a plugin model.
- USI Metadata - The ability to store metadata about a document and stamp the document with an identifier. This identifier can later be read by automated systems and the metadata can be retrieved. The nature and content of the metadata is determined by the needs of the client systems and is controlled by the individual plugins.

The system may process PII related to veterans and dependents. This PII data may be stored by the system in the form of USI Metadata or embedded in generated PDFs.

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 Account Information
☒ Health Insurance Beneficiary Numbers
☒ Account numbers
☒ Certificate/License numbers*
☒ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Current Medications
☒ Previous 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)

- The system does not explicitly collect or use any business data, but plugins developed for the system may. As such, any of this data, if placed on a generated document could pass through the system.
- ADG tracks the file number when batching files for processing.
- PURDG tracks the sender information that will go in an instruction letter (sender name and address) and document types of correspondence received.

PII Mapping of Components (Servers/Database)

Document Generator consists of four key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Document Generator and the reasons for the collection of the PII are in the table below.

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
DocGen Service (microservice)	Yes	Yes	• Name • Social security number • Date of birth • Mothers maiden name • Personal mailing address • Personal phone number • Personal fax number • Personal email address • Emergency contact name • Emergency contact phone number • Financial account information	Placement of information onto a generated document or stored in relation to a USI for use in further downstream processing.	Authentication is required to interact with the Service. API keys are shared with consumers as part of an approval process with the Information Security Officer (ISO). All data traverses the network via SSL (HTTPS). All data is stored in a secured database.

			• Health insurance beneficiary numbers • Account numbers •Certificate/license number • Vehicle license plate number • IP address • Current medications • Previous medical records • Race/ethnicity • Tax identification number • Medical record number		
DocGen Management Tool	Yes	No	• Name • Social security number • Date of birth • Mothers maiden name • Personal mailing address • Personal phone number • Personal fax number • Personal email address • Emergency contact name • Emergency contact phone number • Financial account information • Health insurance beneficiary numbers • Account numbers • Certificate/license number • Vehicle license plate number • IP address • Current medications	As an authorized user makes changes to a template and needs to test them, they can replay a previously generated document that that specific user generated originally.	Users can only replay their own requests, therefore ensuring that they can only see data that they already have access to.

			• Previous medical records • Race/ethnicity • Tax identification number • Medical record number		
ADG-UI (Automated Document Generator – User Interface)	Yes	Yes	• File number	To be able to see the specific data in the ADG admin UI for troubleshooting purposes in production.	No safeguards currently in place. File number PII is very limited as it is not coupled with any other PII so no inferences can be made. There is no external exposure since the service is in the same AWS cluster.
PURDG (Document Generator – plugin for Printing of Unidentified Records	Yes	Yes	• Sender name • Sender mailing address • Document types of correspondence received	Placement of information onto a generated document or stored in a relational database for use in further downstream processing.	Authentication is required to interact with the service. API keys are shared with consumers as part of an approval process with the Information Security Officer (ISO). All data traverses the network via SSL (HTTPS). All data is stored in a secured database.

1.2 What are the sources of the information in the system?

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?

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.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

Data is collected by any application that integrates with the Document Generator. Currently there are no consumers in production. The PIA will be updated when consumers begin interacting with the API.

1.3 How is the information collected?

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

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 technology used in the storage or transmission of information in identifiable form?

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.

Data is not collected by this Service. The means for sourcing the data lie within the client systems that call the DocGen Service.

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.

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

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

The DocGen Service is not responsible for the accuracy of the data. This responsibility lies within the client systems that call the DocGen 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

58VA21/22/28 86 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, 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
- 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

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.

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: Incorrect data could be placed on documents or included in USI Metadata.

Mitigation: Add system controls to validate data inputs; require ISO review and approval for any system to interact with the DocGen Service.

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 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.

The Document Generator has no requirements as to the information it takes in, it takes that information and uploads it to a template and the template can then be used by other services that are developed specifically for the template.

The Document Generator will provide the capability to generate any type of document needed by the business, via the development of plugins. The storage and retrieval of USI metadata will, in the future, support a variety of automation functions, by allowing access to data needed to support those functions without requiring that data to be placed on a document.

DocGen ADG service is a document intake system for handling the ingestion and processing of files, developed to replace the legacy Batch File Interface (BFI) application as a part of the broader efforts to decommission Virtual VA (VVA). ADG – User Interface (ADG-UI) is a multi-faceted admin-facing interface that will allow for the maintaining and updating of the ADG system via a convenient web application. ADG itself does not handle any of the specific documents and is instead an orchestration system that oversees the flow of documents form the batches into the processing system. ADG-UI will provide metrics for processed batches, allow targeted retrying or manual filling of any failed or otherwise unsuccessful batch files, and allow for the creation and updating of pre-defined batch file routines.

The DocGen-plugin for Printing of Unidentified Records (PURDG) only stores DocGen-plugin profile information in the PUR database. The DocGen plugin will contain a template of the instruction letter. Information will be passed to the DocGen-plugin to populate the instruction letter and a pdf document will be generated. This document will be stored in the Claim Evidence S3 bucket. The generated instruction letter will be packaged with the scanned mail items and mailed back to the sender.

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.

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.

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.

Monitoring is accomplished using Prometheus & Grafana. They system is configured to monitor CPU, memory, I/O, API request/response latency and API HTTP response codes. Alerts are configured to notify administrators if the application is having resource (e.g. memory or cpu) issues.

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?

Data is stored in AWS where Industry standard encryptions are present for both in transit and at rest information.

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

Authority to collect should be inherited from the systems that call Document Generation Service to generate a document. No user can retrieve the information from application directly.

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.

The SORN defines the information collected from Veterans, use of the information, and how the information is accessed and stored.

To receive access to the Document Generator a partner (i.e. client application) will need approval from the Document Generator Information System Owner. A unique application key will be created for the partner to access the Service. The key is provided for every request to access the Service.

Documentation is provided to partners prior to using the Service and integration testing must be completed and signed off by the API Information System Owner prior to granting application keys to use the Service.

2.4a How is access to the PII determined?

Users must be registered within VA systems to access and user must be authorized based on user roles to access any and all information.

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. Data modifications are audited. The application is used to display PII and is transmitted via SSL encrypted networks. Access to the data is restricted to logged in users with the proper authorization to view.

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

VBA end users of the system must take annual FTI awareness and protection training as outlined in IRS Publication 1075. This training must be completed via the VA's Talent Management System 2.0 (TMS) and compliance is tracked through the TMS 2.0 system. Section3. Retention of Information.

Section 3. Retention of Information

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

3.1 What information is retained?

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

USI Metadata – a set of name/value pairs as defined by the client applications.
Generated Documents

Name
Sender name
Social security number
File number
Date of birth
Mother's maiden name
Personal mailing address
Sender mailing address
Personal phone number
Personal fax number
Personal email address
Emergency contact name
Emergency contact phone number
Financial account information
Health insurance beneficiary numbers
Account numbers
Certificate/license number
Vehicle license plate number
IP address
Current medications
Previous medical records
Race/ethnicity
Tax identification number

Medical record number
Document types of correspondence received

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.

USI Metadata is retained indefinitely.

A copy of generated documents may be stored for a limited time (up to 90 days) for troubleshooting, analysis and Validation purposes.

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.
This question is related to privacy control DM-2, Data Retention and Disposal

No information is retained via personal identifiers.

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_I.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.

Generated documents will be purged from the system on a daily basis. Any documents older than the retention period will be removed.

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.

Yes. No PII data is used in testing or development environments. Only production system admins have access to production environments.

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.

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: USI data is stored indefinitely
Mitigation: Access to USI data is controlled via application permissions.

Privacy Risk: Documents are stored
Mitigation: Only users who created the documents can access them. Documents are purged after 90 days.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information

transmitted? NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Office of Information and Technology	va.gov – future connectivity plans. Currently not connected.	• Name • Sender name • Social security number • File number • Date of birth • Mothers maiden name • Personal mailing address • Sender mailing address • Personal phone number • Personal fax number • Personal email address • Emergency contact name • Emergency contact phone number • Financial account information • Health insurance beneficiary numbers • Account numbers	HTTPS Request/Response (JSON data format)

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*
		• Certificate/license number • Vehicle license plate number • IP address • Current medications • Previous medical records • Race/ethnicity • Tax identification number • Medical record number • Document types of correspondence received	

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.
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 SPI 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 for the system. Further, SPI will be encrypted in transit and at rest.

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				

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

Document Generator does not share data with third parties.

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, as there is no sharing of information outside of VA with external parties

Mitigation: Not applicable, 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.

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.

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

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 for the collection of Personally Identifiable Information is outlined in SORN 58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

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.

It is the responsibility of client applications (e.g. mobile or web application) that integrate with the Document Generator to provide the opportunity to decline providing information.

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.

It is the responsibility of client applications (e.g. mobile or web application) that integrate with the Document Generator to provide the opportunity to consent to a particular use of information collected.

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.

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: The Document Generator does not know how client applications will use the data retrieved from the API.

Mitigation: The Document Generator should be added as an internal integration partner as part of the PIA or PTA for any application that integrates with the API.

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.

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.***

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).

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.

Procedures for individuals to gain access to their information is described in SORN 58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

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 for records can be submitted by following procedures outlined in SORN 58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

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 notified of procedures for correcting their information via SORN published in the Federal Register (SORN 58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA).

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.

Formal redress procedures are published in the Federal Register per SORN 58VA21/22/2886 FR 61858 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA.

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.***

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

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

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

Follow the format below:

Privacy Risk: There is a risk that a system provides incorrect information to the Document Generator to create/update claims or contentions.

Mitigation: The Document Generator will include data validation and will provide error messages to client applications if data is invalid or fails business rule processing. It is a responsibility of integration partners to handle errors and present data to end users in a reliable way. Corrections should be handled by the customer facing application.

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.

Describe the process by which an individual receives access to the system.

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?

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.

To receive access to the Document Generator a partner (i.e. client application) will need approval from the Information System Owner. A unique application key will be created for the partner to access the API.

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.

Contractor teams support the BIP production environment and as such has access to the Document Generator. This includes PII and VA Sensitive Information. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS). The System Administrators will maintain users, update applications and components, introduce new functionality, govern deployment activities and ensure user operability. The System Administrators are not primary users of the Document Generator nor do they development components for the API.

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?

If Yes, provide:

1. *The Security Plan Status:* Not yet approved
2. *The System Security Plan Status Date:* n/a
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 12/21/22
5. *The Authorization Termination Date: 12/21/23*
6. *The Risk Review Completion Date:* 5/25/23
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.

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)*

DocGen utilizes the VA Enterprise Cloud (VAEC)is FedRAMP approved operating on a Platform as a service model.

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

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

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

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

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

ID	Privacy Controls
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.

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2023.09.12 12:58:39 -06'00'

Privacy Officer, Jean-Claude Wicks

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2023.09.15 09:16:20 -04'00'

Information System Security Officer, Joseph Facciolli

Christina O. Lawyer 141790

Digitally signed by Christina O. Lawyer 141790
Date: 2023.09.18 09:24:49 -04'00'

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).

Notice of Privacy Practices This system is intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA; all use is considered to be understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms. Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties. PRIVACY ACT INFORMATION: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA Programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain or retain benefits. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us, your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefit for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine maximum benefits under the law. The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies.

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