



Privacy Impact Assessment for the VA IT System called:

Electronic Insurance (EIN)

EPMO/EPMD/BAM/Insurance Product Line

VBA

Date PIA submitted for review:

5/31/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jason Anderson	jason.anderson3@va.gov	(202) 570-0255
Information System Security Officer (ISSO)	Dingle, Calvin	Calvin.dingle@va.gov	8037764000x4835
Information System Owner	Ritenour, Theodore J.	Theodore.Ritenour@va.gov	303-594-8935

Abstract

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

Electronic Insurance (EIN) is the veteran web-facing component which enables the veterans to apply for life insurance benefits and then helps process the applications.”

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.*
Electronic Insurance (EIN). Enterprise Program Management Office (EPMO) / Enterprise Portfolio Management Division (EPMO) / Benefits and Memorial Services (BAM)/Insurance Product Line

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

The mission of VA's insurance program is "to provide life insurance benefits to veterans and service members not available from the commercial insurance industry due to lost or impaired insurability resulting from military service." The Insurance Center relies on Electronic Insurance IT infrastructure to support systems that meet or exceed all insurance industry performance standards in timeliness, accuracy, and customer satisfaction.

C. *Indicate the ownership or control of the IT system or project.*
Ritenour, Theodore J. <Theodore.Ritenour@va.gov>

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.*

6.1 million veterans and members of the uniformed services

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

The Veteran facing portions of Electronic Insurance are websites housed within the Philadelphia ITC (PITC) DMZ. These systems act as an entry point to VA Life Insurance Self Service web applications. These components are part of the Veteran facing Insurance Self-Service System: Online Policy Access (OPA) - OPA allows users to view their insurance policy information and documents, request a policy loan or dividend withdrawal. It is integrated with Identity Access Management Access VA service to provide Level 2 authentication to users who wish to view their policy information online. Unclaimed Funds

Search (UFN) - UFN allows the public to search a database of unclaimed funds by name, social security number or other identifying data to see if Insurance might be holding a returned check or other unclaimed liability. Service-Disabled Veterans Insurance (S-DVI) - S-DVI allows veterans with a rating for a new disability to apply for Service-Disabled Veterans Insurance online. Applicants can submit their applications electronically or print and mail their completed application. The on-line form uses turbo-tax type questions to help determine eligibility. Its data output creates the Veterans Insurance Claims Tracking and Response System (VICTARS) record for immediate processing.

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

The internal web portions of Electronic Insurance utilized by VA personnel are housed at the PITC behind the DMZ and on the internal VA Insurance network locations. These components are part of the internal VA Insurance web system: Insurance Collections - An online portal for processing Veteran policy payments used internally by Insurance specialists. Contains tools for processing via Pay.gov for Pre-Authorized Debits (PADS) and for online bill pay via the US banking system. Insurance Dashboard - Provides an area for web-based reports and other internal administrative functions as needed. Insurance Service API - REST based web service to provide common access point for Insurance business functionality. Provides ability to expand and consolidate functionality when required by the Insurance business.

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

N/A

3. Legal Authority and SORN

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

The authority for this interconnection is based on: •Federal Information Security Management Act (FISMA) VA Directive 6500, Managing Information Security Risk: VA Information Security Program, and Handbook 6500, Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program. Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, Security Guide for Interconnecting Information Technology Systems 38 United States Code (U.S.C.) §§ 5721-5728, Veteran’s Benefits, Information Security Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Systems, 18 U.S.C. 641 Criminal Code: Public Money, Property or Records 18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information, 38 U.S.C. 1965 – 1980A: Subchapter III—Servicemembers’ Group Life Insurance, 38 Code of Federal Regulations (C.F.R.) Part 9 SGLI Group Policy G-32000 and any amendments/modifications agreed to by VA and Prudential The authority to disclose VA data per this agreement must comply with disclosure authority under each of these applicable statutes: Privacy Act of 1974, 5 U.S.C. § 552a Confidential Nature of Claims, 38 U.S.C § 5701 Confidentiality of Certain Medical Records, 38 U.S.C. § 7332

Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. § 5705 Freedom of Information Act, 5 U.S.C. § 552 Authority for Maintenance of the System: Title 38, United States Code (U.S.C.), chapter 5, section 501, and chapter 3, including sections 303 and 315, Title 38, U.S.C., chapter 19; chapter 21, section 2106; and Title 5 U.S.C. *Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance* — The system SORN is 36VA29 8/30/2018 <https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf>; in the Federal Register (83 FR 44407) and online.

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

D. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

Version Date: October 1, 2022

Page 3 of 34

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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

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

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>

None

PII Mapping of Components (Servers/Database)

Electronic Insurance consists of 4 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Electronic Insurance and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. **The first table of 3.9 in the PTA should be used to answer this question.**

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
Insurance Database	Yes – stores	Yes	Name SSN DOB Mailing Address Email address Phone number	To provide and manage benefits for the Veteran’s policy(ies)	System user access is permitted only with use of the PIV card and authorized user of the SQL database.
Online Policy Access	Yes – collects	Yes	Name SSN DOB Mailing Address Email address Phone number	For online acceptance of Beneficiary designation	System access only available to users with AccessVA account.
S-DVI	Yes – collects	Yes	Name SSN DOB Mailing Address	To manage Service Disabled Applications collected online and processed	System access only available to users

			Email address Phone number	thru the Veterans Insurance Claims Tracking and Response System VICTARS record	with AccessVA account.
--	--	--	---	---	---------------------------------------

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?

The veteran, member of the uniformed services, or someone acting on their behalf; the uniformed services, other federal agencies, including the Department of Defense (DoD); Social Security Administration (SSA); U.S. Treasury Department; Office of Service members' Group Life Insurance (OSGLI); State and local agencies; Federal, State, and local courts; VA records; VA and private physicians; VA and private medical facilities; accredited veterans service organizations and other organizations aiding veterans and members of the uniformed services; VA-approved claims agents; VA fiduciaries; court-appointed guardians/conservators, powers of attorney, and military trustees; financial institutions; beneficiaries; commercial insurance companies; undertakers; lending institutions holding a veteran's or uniformed services member's mortgage; VA Loan Guaranty records; contractors remodeling or enlarging or adding construction to existing homes; relatives and other interested persons; West Group public records commercial database; Inquiry Routing & Information System (IRIS); and the general public.

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.

Social Security Administration provides information related to notice of death for a particular veteran. VAProfile validates Veterans eligibility.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

VAProfile, Social Security Administration and Treasury Department

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?

Some data is collected directly from Veterans when logged into the Online Policy Access or S-DVI system. These areas of the system are protected by the AccessVA identification portal prior to information transference and storage.

The majority of system data is electronically transferred to the Electronic Insurance System from internal VA Insurance policy administration systems. This data is not collected directly from individuals but is electronically transferred from Insurance and US Government systems such as:

- Insurance General Support Systems (GSS)
 - Veterans Insurance Claims Tracking and Response System (VICTARS)
 - Insurance Payment System (IPS)
 - Data interchange with Department of Treasury to GSS – to process disbursements and returned items. This data is received in Philadelphia over a dedicated line from Treasury that utilizes their approved encryption

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

N/A

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

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

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

The information is checked for accuracy by reviewing the data provided by veterans and their beneficiaries, who are responsible for the submission of federal and state documents, VA records, and other official materials. Employees also conduct data matching procedures and perform internal audits in order to verify the accuracy of information stored in the system.

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

N/A

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

System Sorn is: 36VA29 8/30/2018 <https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf>; in the Federal Register (83 FR 44407) and online.

The authority for this interconnection is based on:

- Federal Information Security Management Act (FISMA)
- VA Directive 6500, Managing Information Security Risk: VA Information Security Program, and Handbook 6500, Risk Management Framework for VA Information Systems: Tier 3 – VA Information Security Program
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, Security Guide for Interconnecting Information Technology Systems
- 38 United States Code (U.S.C.) §§ 5721-5728, Veteran’s Benefits, Information Security
- Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Systems
- 18 U.S.C. 641 Criminal Code: Public Money, Property or Records
- 18 U.S.C. 1905 Criminal Code: Disclosure of Confidential Information
- 38 U.S.C. 1965 – 1980A: Subchapter III—Servicemembers’ Group Life Insurance
- 38 Code of Federal Regulations (C.F.R.) Part 9
- SGLI Group Policy G-32000 and any amendments/modifications agreed to by VA and Prudential

The authority to disclose VA data per this agreement must comply with disclosure authority under each of these applicable statutes:

- Privacy Act of 1974, 5 U.S.C. § 552a
- Confidential Nature of Claims, 38 U.S.C § 5701
- Confidentiality of Certain Medical Records, 38 U.S.C. § 7332
- Confidentiality of Healthcare Quality Assurance Review Records, 38 U.S.C. § 5705
- Freedom of Information Act, 5 U.S.C. § 552

Authority for Maintenance of the System: Title 38, United States Code (U.S.C.), chapter 5, section 501, and chapter 3, including sections 303 and 315, Title 38, U.S.C., chapter 19; chapter 21, section 2106; and Title 5 U.S.C. *Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance* — 36VA29 8/30/2018 <https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf>; in the Federal Register (83 FR 44407) and online.

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: Sensitive Personal Information including personal contact information, service information and benefit information may be released to unauthorized individuals.

Version Date: October 1, 2022

Page 9 of 34

Mitigation: The Electronic Insurance adheres to information security requirements instituted by the VA Office of Information Technology (OIT).

- All employees with access to a veteran's information are required to complete the VA Privacy and Information Security Awareness Training and Rules of Behavior annually.
- The MS-Outlook default setting is configured to encrypt all email messages.

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 Electronic Insurance system collects personal information that is necessary to determine life insurance related benefits for veterans and service members. For example: veteran personal data (Name, Address, Social Security Number, Family/Dependents, Marital Status, Medical Status, Service information, Birth Information, Death Information) and veteran dependent personal data including name and address, Social Security Number, age, relationship to the veteran is used to communicate with the veteran/dependent about his/her benefits, to notify of change in account status and advise about new options. Insureds and beneficiary's name, address, bank data (optional), telephone number (optional), and email address(optional) may also be collected; this information is used to contact the veteran policyholder on a scheduled basis in order to pay annual dividends, inform the veteran of new or changes in benefits, advise of changes to policy status, or request repayment of a loan or lien, or to perform outreach services.

The information in the system will be used in support of the program's business purpose by enabling the Electronic Insurance system to provide the following to Veterans and the public (i.e. external uses):

- Ability to view Insurance benefits online and manage aspects of policy to include loan requests and dividend payment management
- To apply for S-DVI policies
- Find information on policies that have not paid out benefits in the form of unclaimed funds

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.

Any newly derived information may be placed in an individual's existing record. New records are generated only in response to new claims or new applications for an insurance benefit. The records, whether new or existing, are only accessible to government employees, and contractors, who are authorized to have such access on a need-to-know basis.

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

The system is capable of generating statistical analysis and reports that detail various insurance programs activities and features, such as the number of insureds in a program, premium rates, loan value, and activities processed in the records and payments received.

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 both at rest and in transit. Retention is stored in database encrypted.

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

SSNs are only used on the server to identify the veteran. Once provided, the SSN is masked on the web side.

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

Retention is stored in database encrypted.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

All employees with access to a veteran's information are required to complete the VA Privacy and Information Security awareness training and Rules of Behavior annually. Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination. Individual users are given access to a veteran's data through the issuance of a user ID and password and using a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user's user ID limits the access to only the information required to enable the user to complete their job-related duties. The Insurance Center System of Records Notice (SORN), also known as the Veterans and Uniformed Services Personnel Programs of US Government Life Insurance-VA (36VA29), available at Federal Register at 75 FR 65405 and online at <https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf> provides a detailed explanation of the ways information is collected and used based on the mission of the VA Insurance Center.

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?

ISO

Section 3. Retention of Information

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

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

The information is retained on a database server identified as VBAINSSQLP12 within the boundary of Electronic Insurance. The information collected and stored is Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number, and Email Address.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.

VBAINSSQLP12, the database system for the insurance programs, maintains imaged insurance records indefinitely. Back-up VA Philadelphia Information Technology Center (PITC) archive records are stored on tape for one year prior to being erased or written over.

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.

Version Date: October 1, 2022

Page 13 of 34

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.

Records Control Schedule VB-1 Part 1, Section, XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB-1, Part 1, Section VII

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.

According to the OIT OIS SOP Media Sanitation SOP page 4 “6.2 Media Sanitization. All media for disposition that is not Federal Information Processing Standards (FIPS) 140-2 encrypted must be sanitized and/or extensively damaged before delivery to the nationally approved media disposition vendor.”

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.

When used for testing purposes the data identified as PII is obfuscated within those test and training 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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that the information contained in the system will be retained for longer than is necessary to fulfill the mission of the Electronic Insurance System.

Mitigation: Information contained in the EIN system is only accessible for the life span of either the insured or the policy being enforced. When VA Life Insurance is notified of either of these events, the account will no longer be accessible from online tools. After an award is paid, the inactive records are archived to tape and taken to the off-site location in Iron Mountain. Active records that remain will be secured and monitored in accordance with utilizing VA policy. RCS VB- Part II Revised for VBA

<http://www.benefits.va.gov/warms/docs/admin20/rcs/part2/vb-1partii.doc> All personnel with access to the veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. EIN adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).

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
Philadelphia Information Technology Center (PITC) VBAINSSQLINS	Physical location of Electronic Insurance system	Name Social Security Number, DOB, Mailing Address, Email Address, Phone Number	LAN, HTTPS
Veterans Benefits Administration, VA Insurance Center VBAINSSQLINS	For use within the VA Insurance business	Name Social Security Number, DOB, Mailing Address, Email Address, Phone Number	LAN, HTTPS
Identity Access Management (IAM)	For use within the VA Insurance business	Single Sign On external (SSOe) – Veteranemail address, security identifier (SECID), group/role memberships.	LAN, HTTPS
VA Profile	For use within the VA Insurance business	Service-connected indicator	LAN, HTTPS

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: Privacy information may be released to unauthorized individuals.

Mitigation: All personnel with access to a veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. Persons with access to the VAIC systems are authorized only based on the use of their PIV card and related password(s). Information sharing internally is permitted among persons who have a “need to know basis” and system access is limited to authorized persons only. The Electronic Insurance system adheres to all information security requirements instituted by the VA Office of Information Technology (OIT). Information is shared in accordance with VA Handbook 6500.

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

Version Date: October 1, 2022

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>
Department of Treasury	Financial Accounting with/for Insurance Claims	name, billing address, email, policy number	ISA/MOU	HTTPS

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: Disclosure of PII during transmission between VA and Department of Treasury

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.

For Death Benefit related forms:

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 identified in the VA system of records, 36VA29, Veterans and Armed Forces Personnel U.S. Government Life Insurance Records - VA and published in the Federal Register. Your obligation to respond is required to obtain this benefit.

RESPONDENT BURDEN: We need this information to determine your eligibility for a death benefit (Death benefit indicator from VAF 29-541). Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 30 minutes to review the instructions, find the information, and complete this form. VA cannot conduct or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet page at <http://www.reginfo.gov/public/do/PRAMain>. If desired, you can call 1-800-827-1000 to get information on where to send comments or suggestions about this form.

For Live Benefit related forms:

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 identified in the VA system of records, 36VA29 8/30/2018 <https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018->

[18789.pdf](#) , Veterans and Armed Forces Personnel U.S. Government Life Insurance Records - VA and published in the Federal Register. Your obligation to respond is required to obtain this benefit. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law in effect prior to January 1, 1975, and still in effect.

RESPONDENT BURDEN: We need this information to determine your eligibility for VA insurance benefits. Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 1 hour and 45 minutes to review the instructions, find the information, and complete this form. VA cannot conduct or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet page at www.reginfo.gov/public/do/PRAMain. If desired, you can call 1-800-827-1000 to get information on where to send your comments or suggestions about this form.

PRIVACY ACT NOTICE: 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 identified in the VA system of records, 36VA29 8/30/2018 <https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf>, Veterans and Armed Forces Personnel U.S. Government Life Insurance Records - VA and published in the Federal Register. Your obligation to respond is voluntary, but your failure to provide us the information could impede processing. Giving us your Social Security number (SSN) account information is mandatory. Applicants are required to provide their SSN. VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law in effect prior to January 1, 1975, and still in effect. The responses you submit are considered confidential (38 U.S.C. 5701).

RESPONDENT BURDEN: We need this information to ensure proper transmission of your funds via electronic transfer to your financial institution (31 CFR 208.3 and 210.4). Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 20 minutes to review the instructions, find the information, and complete this form. VA cannot conduct or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet page at www.reginfo.gov/public/do/PRAMain. If desired, you can call 1-800-827-1000 to get information on where to send comments or suggestions about this form

The Insurance Center also provides notice by publishing the VA System of Record Notice (SORN

), also known as the *Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance* — 36VA29 8/30/2018 <https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf>; in the Federal Register (83 FR 44407) and online.

This Privacy Impact Assessment (PIA) also serves as notice of the Electronic Insurance System. As required by the eGovernment Act of 2002, Public Law 107-347208(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”.

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

<https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.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 notice directs individuals who desire to gain access to their records to write to the Insurance Center at 5000 Wissahickon Avenue, P.O. Box 8079, Philadelphia, PA 19101.

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.

An individual may always decline to provide information; however, if the requested information is considered relevant and necessary to determine eligibility for an insurance benefit, then a refusal to provide the necessary information may result in denial of the requested benefit. (38 U.S.C. 5101).

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.

Any individual who wishes to determine whether a record is being maintained in the Insurance System of Records under his or her name or other personal identifier, or who wants to determine the contents of such record, or has a routine inquiry concerning the status of his or her insurance under this system may contact the VA Insurance Center in Philadelphia, Pennsylvania at (215) 381-3029. Requests concerning the specific content of a record must be made in writing or made in person to the VA Insurance Center in Philadelphia, Pennsylvania. The inquirer should provide the full name of the veteran or member of the uniformed services, their insurance file number or VA claim number or social security number, the date of birth of the veteran or member of the uniformed services, and reasonably identify the benefit or system

of records involved. If the insurance file number or any of the other identifiers noted above are not available, the service number, and/or location of insurance records that will aid VA personnel in locating the official insurance records should be provided. The Insurance System of Records Notice (SORN) provides that an individual generally must consent to each use of the information in his insurance record; however, the SORN also lists exceptions to when the individual's consent is not required, such exceptions are listed as "routine uses" in the SORN and are clearly identified.

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: Privacy information may be collected prior to providing the written notice.

Mitigation: The VA mitigates this risk by providing veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The 3 main forms of notice are discussed in detail in question 6.1 and include the Privacy Act Statement, a Systems of Record Notice (SORN), and the publication of this Privacy Impact Assessment (PIA)

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.

As specified in the Insurance SORN, the Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance -36VA29), individuals who desire to gain access to their records should write to the Insurance Center at 5000 Wissahickon Avenue, P.O. Box 8079, Philadelphia, PA 19101.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

N/A

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

N/A

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The following procedure is from VA Handbook 6300.4: (1) An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the requirements in paragraph 3b(3) of this Handbook. It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester should be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired. (2) Not later than 10 days, excluding Saturdays, Sundays, and legal public holidays, after the date of receipt of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination has not been made, the acknowledgement will inform the individual when he or she may expect to be advised of action taken on the request. VA will complete a review of the request to amend or correct a record as soon as reasonably possible, normally within 30 days from receipt of the request (excluding Saturdays, Sundays, and legal public holidays). (3) Where VA agrees with the individual's request to amend his or her record(s), the requirements of 5 U.S.C. 552a(d) will be followed. The record(s) will be corrected promptly and the individual will be advised promptly of the correction. Amendment consists of adding information to the record, altering information in the record, or deleting information in the record. Under the Privacy Act, if information is altered or deleted, the previous version must be obliterated and illegible after amendment. The amendment should be annotated "Amended, Privacy Act, (date), (signature and title of amending official)." (4) If the record has previously been disclosed to any person or agency, and

an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. FL 70- 19, Notification to Other Person or Agency of Amendment to a Record, may be used. (5) If it is determined not to grant all or any portion of the request to amend a record, the official will promptly notify the individual in writing. The individual will be advised of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The notice will specify the reason(s) for denying the request, identify the VA regulations or statutes upon which the denial is based, and advise that the denial may be appealed in writing to the General Counsel (024), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. FL 70-20, Notification of Initial Refusal to Amend a Record under the Privacy Act, may be used for this purpose. (6) The determination on an appeal will be made not later than 30 days, excluding Saturdays, Sundays, and legal public holidays, from the date the individual's letter of appeal is received unless the Secretary or Deputy Secretary, for good cause shown, extends such 30-day period. If the 30-day period is so extended, the individual will be notified promptly of the reasons for the extension and the date on which a final determination may be expected. The final determination in such appeals will be made by the General Counsel or Deputy General Counsel. (7) If the General Counsel or Deputy General Counsel finds that the adverse determination should be reversed, he or she will notify the VA office or station of the remedial action to be taken. The VA office or station will promptly carry out that action. The General Counsel or Deputy General Counsel will promptly notify the individual in writing of the corrective action. The field station or Central Office organization that provided the initial decision will inform previous recipients of the record that a correction has been made. (8) If the General Counsel or Deputy General Counsel determines that the adverse determination will not be reversed, the individual will be notified promptly in writing of that determination, the reasons therefor, and of his or her right to seek judicial review of the decision pursuant to section 3 of the Privacy Act (5 U.S.C. 552a(g)). (9) If the adverse determination is sustained by the General Counsel or Deputy General Counsel, the individual will also be advised promptly of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The statement may contain information that the individual believes should be substituted. (10) When an individual files a statement disagreeing with VA's decision not to amend a record, the record will be clearly annotated so that the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose it. When the disputed record is disclosed to persons or other agencies, the fact of the dispute will be clearly noted. Copies of the statement of disagreement will be provided, and, when appropriate, copies of a concise statement of VA's reasons for not making the amendment(s) requested will also be provided. (11) A decision by either the General Counsel or Deputy General Counsel pursuant to paragraph 3f (7) of this Handbook is final. It is subject to judicial review in the district court of the United States in which the complainant resides, or has his or her principal place of business, or in which the VA records are located, or in the District of Columbia

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.

Veterans and their beneficiaries are notified of the procedures for correcting their records at the Insurance Center through the VA System of Records Notice (SORN), also known as the Veterans and Uniformed Services Personnel Programs of US Government Life Insurance - 36VA29. Based on the SORN's Records Access Procedure—individuals desiring access to, and who wish to contest information in their VA insurance records and learn more about related

procedures should write to the Insurance Center at 5000 Wissahickon Ave, PO Box 8079, Philadelphia, PA 19101.

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.

Individuals desiring access to, and who wish to contest information in, their VA insurance records and learn more about related procedures should write to the Insurance Center at 5000 Wissahickon Ave, PO Box 8079, Philadelphia, PA 19101.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: *Is the individual provided with the ability to find out whether a project maintains a record relating to him?*

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

Principle of Individual Participation: *Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?*

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information

Mitigation: This privacy risk is mitigated by information provided in the Electronic Insurance SORN (*Veterans and Uniformed Services Personnel Programs of US Government Life Insurance—36VA29*)), Records Access Procedure which states that individuals desiring access to, or wishing to

contest information, in their insurance records can write to the Insurance Center at 5000 Wissahickon Ave, PO Box 8079, Philadelphia, PA 19101.

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.

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls. OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring are performed through the use of VA's Talent Management System (TMS). Individuals are subject to a background investigation before they are given access to a veteran's information. All personnel with access to a veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. Employees with access to sensitive information are provided access based on their position requirements where such access is only obtained using a Personal Identity Verification (PIV) card and/or password authentication. This ensures the identity of the user by requiring two-factor authentication when required. The user's ID limits the access to only the information required for the user to complete their job-related duties.

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?

N/A

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.

N/A

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.

Contractors will have access to the system after completing the VA Privacy and Information Security Awareness training and Rules of Behavior annually, and after the initiation of a background investigation. All system access is reviewed on a Monthly, Quarterly, Semi-Annually, and Annual basis depending on type of account. Accounts are reviewed by supervisors, and FISO. Contractors with access to sensitive information are provided access based on their position requirements where such access is only obtained using a Personal Identity Verification (PIV) card and/or password authentication. This ensures the identity of the user by requiring two-factor authentication when required. The user's ID limits the access to only the information required for the user to complete their job-related duties. Contracts are reviewed evaluated by the ISO and Privacy Officer prior to implementation.

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.

Yes, there are contract system administration personnel within the Philadelphia Information Technology Center (PITC) who maintain the server hardware and software but are not primary users of the EIN system itself. VA requires Privacy and Information Security Awareness training be completed on an annual basis. The Talent Management System offers the following applicable privacy courses: VA 10176: Privacy and Information Security Awareness and Rules of Behavior, VA 10203: Privacy and HIPAA Training, and VA 3812493: Annual Government Ethics

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

8.4a If Yes, provide:

- 1. The Security Plan Status: Complete*
- 2. The System Security Plan Status Date: 5/11/2023*
- 3. The Authorization Status: Authorized to Operate*

4. *The Authorization Date: 4/21/2023*
5. *The Authorization Termination Date: 7/23/2023*
6. *The Risk Review Completion Date: 5/11/2023*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Moderate*

Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.

*8.4b If No or In Process, provide your **Initial Operating Capability (IOC) date.***

EIN currently has 3 Months (90 days) ATOC, this ATO will expire on July 23, 2023. FIPS 199 classification is MODERATE

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)

No

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.

N/A

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.

N/A

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.

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	Authority and Purpose
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	Accountability, Audit, and Risk Management
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development

ID	Privacy Controls
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, Jason Anderson

Information System Security Officer, Calvin Dingle

Information System Owner, Theodore Ritenour

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). 36VA29 8/30/2018
<https://www.govinfo.gov/content/pkg/FR-2018-08-30/pdf/2018-18789.pdf> , Veterans and Armed Forces Personnel U.S. Government Life Insurance Records forms.

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](#)