



Privacy Impact Assessment for the VA IT System called:

Enrollment Database (EDB)

Veterans Health Administration (VHA)

Enrollment Health Benefit Determination (EHBD)

eMASS ID 109

Date PIA submitted for review:

9-19-2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Shirley Hobson	Shirley.Hobson@va.gov	404-828-5337
Information System Security Officer (ISSO)	Howard Knight	Howard.Knight@va.gov	404-828-5340
Information System Owner (ISO)	Temperance Leister	Temperance.Leister@va.gov	484-432-6161

Abstract

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

Enrollment Database (EDB) uses Federal Tax Information (FTI) to conduct Means Testing and Income Verification Matching to determine the level of medical care benefits package from VA.

Overview

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

1 General Description

- A. *What is the IT system name and the name of the program office that owns the IT system?*

Enrollment Database (EDB); Enrollment Health Benefit Determination (EHBD) - Health Eligibility Center (HEC) Income Verification Division (IVD) office which is part of the Enrollment Health Benefit Determination (EHBD) program.

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

Enrollment Database (EDB) is a web-based application for the Health Eligibility Center (HEC) in Atlanta, Georgia. Income Verification Division (IVD) analysts at HEC use EDB to perform annual income verification of Veterans for eligibility. HEC performs yearly Means Tests on all Veterans whose eligibility is based on income. Each year analysts take the data reports by Veterans and compare it to information received from IRS and SSA to determine an individual Veteran’s eligibility. The Means Test results are reported back to the Veteran’s VA Medical Center treating facility. The EDB application produces letter correspondence to assist IVD analysts in gathering information from Veterans and to inform Veterans of any changes in their eligibility status.

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

VA Owned and VA Operated information system (IS)

2. Information Collection and Sharing

- D. *What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*

The expected number of individuals whose information is being used in the system is 12 million. EDB performs yearly Means Test on all Veterans whose eligibility is based on income. VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service members, reservists, their spouses and their dependents, who file claims for a wide variety of Federal Veteran’s benefits administered by VA.

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

EDB contains demographic and financial data. EDB sends and receives Federal Tax Information (FTI) from the Internal Revenue Service and Social Security Administration. This FTI is used to conduct Means Testing and Income Verification Matching to determine the level of medical care benefits package from VA. Information derived from FTI is used to support decision information to the VA Medical Center facilities.

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

EDB shares data externally with Social Security Administration (SSA) and Internal Revenue Service (IRS). EDB also communicates internally with Veterans Data Integration & Federation (VDIF) which sends information on to VA Medical centers. Data from EDB is used by Veterans Health Administration (VHA) Enrollment System (VES) as part of its Enrollment and Eligibility Service. In addition, data is sent to HEC's print server for letter generations for written correspondence with Veterans.

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

EDB is a web-based application housed at Austin Information Technology Center (AITC) located at 1615 Woodward St. Austin, TX 78772. Access is limited to the VA Intranet and customer use by HEC IVD staff is controlled within the application. The data connection between Austin, TX and HEC is an internal connection through the VA network. The servers accessing the data have server certificates issued through the VA Public Key Infrastructure (PKI) and VeriSign. Data passed from server to end customer is through secure client-server communications via the Secure Sockets Layer (SSL) protocol.

3. Legal Authority and SORN

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

System of Record Notice (SORN) is "Income Verification Records-VA" (89VA10). Veterans' Health Care Eligibility Reform Act of 1996, Public Law 104-262; Title 38 U.S.C. Sections 1705, 1710, 1712 and 1722; Title 38 U.S.C Sections 5317 and 5319; Title 26 U.S.C. Section 6103 (I)(7) provide the legal authority for operating the EDB components.

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?

SORN does not require amendment nor does the system use cloud technology.

4. System Changes

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

No.

K. Will 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?

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

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

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

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

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

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

Other PII/PHI data elements: Tax returns, Income for each year Veteran enrolled, Employer information, Eligibility Status, Enrollment Status.

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

PII Mapping of Components (Servers/Database)

Enrollment Database (EDB) consists of **three** key components (servers/ databases/ instances/ applications/ software/ application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **EDB** and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name that contains PII/PHI	Does this system collect PII?	Does this system store PII?	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Database	No	Yes	<p><u>Identity information:</u> Name, Social Security Number (SSN), date of birth, gender, address and e-mail information.</p> <p><u>Financial information:</u> Tax Identification Number (TIN), tax returns, and income for each year Veteran enrolled.</p> <p><u>Military service information:</u> branch of service, discharge type and discharge date.</p> <p><u>Veteran associates:</u> next of kin, family members, their contact information and dependent information.</p> <p>Eligibility status, enrollment status, demographic information, dependents and employer information.</p> <p><u>Internal (Z09) information:</u> Veteran National Integrated Control Number (ICN), Veteran ICN CheckSum, bill amount, billing class, billing type, billing From date, billing To date, transaction code, transaction date, and transaction type.</p>	Means Testing and Income Verification Matching	Restricted user access list, Personal Identity Verification (PIV) authentication
Application	Yes	No	<p><u>Identity information:</u> Name, Social Security Number (SSN), date of birth, gender, address and e-mail information.</p> <p><u>Financial information:</u> Tax Identification Number (TIN), tax</p>	Means Testing and Income Verification Matching	Restricted user access list, Personal Identity Verification

			<p>returns, and income for each year Veteran enrolled.</p> <p><u>Military service information</u>: branch of service, discharge type and discharge date.</p> <p><u>Veteran associates</u>: next of kin, family members, their contact information and dependent information.</p> <p>Eligibility status, enrollment status, demographic information, dependents and employer information.</p> <p><u>Internal (Z09) information</u>: Veteran National Integrated Control Number (ICN), Veteran ICN CheckSum, bill amount, billing class, billing type, billing From date, billing To date, transaction code, transaction date, and transaction type.</p>		(PIV) authentication
Bi-directional	No	No	<p><u>Identity information</u>: Name, Social Security Number (SSN), date of birth, gender.</p> <p>Number of dependents.</p> <p>Eligibility status, enrollment status, EDB Calculations [Means test, Means threshold amount and income]</p>	Means Testing and Income Verification Matching information sharing with other VA application.	Restricted user access list, Personal Identity Verification (PIV) authentication

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?

PII is pulled via Veterans Data Integration & Federation (VDIF) into Enrollment Database to ensure the right information is being used to analyze and verify Veterans enrollment eligibility within the VHA healthcare system. Federal Tax Information (FTI) is received from Internal Revenue Service (IRS) and Social Security Administration (SSA). Information is also gathered through letter correspondence with Veterans.

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.

FTI received from IRS and SSA is used to conduct Means Testing and Income Verification Matching to determine level of medical care benefits package from VA. Information derived from FTI is used to support decisions information to the VA Medical Center facilities. PII pulled from

VDIF to ensure the right information is being used to analyze and verify Veterans enrollment eligibility.

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

EDB creates its own data by conducting Means Testing and Income Verification Matching based on the FTI data from the IRS and SSA.

1.3 How is the information collected?

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

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

Information is received via electronic transmission from VDIF, IRS and SSA. Letter correspondence is used to gather information from Veterans.

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

VA Form 10-10EZ, OMB Control Number: 2900-0091 - Application for Health Benefits
VA Form 10-10EZ, OMB Control Number: 2900-0091 - Health Benefits Update Form
VA Form 10-10HS, OMB Control Number: 2900-0091 - Request for Hardship Determination
VA Form 10-301, OMB Control Number: 2900-0867 - IRS/SSA Veteran Reported Income
VA Form 10-302, OMB Control Number: 2900-0867 - IRS/SSA Spouse Reported Income
VA Form 10-302a, OMB Control Number: 2900-0867 - Spouse Additional Income Information
VA Form 10-303, OMB Control Number: 2900-0867 - Declaration of Representative
VA Form 10-304, OMB Control Number: 2900-0867 - Waiver Statement

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.

Information imported to EDB has its accuracy verified by the original source; VDIF, IRS and SSA data is presumed to be accurate upon import by EDB. Information provided by individuals through correspondence is presumed accurate as it is from the authoritative source. Prior to any award or entitlement authorization(s) by EDB, the veteran record is manually reviewed and data validated to ensure correct entitlement has been approved.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

Each year analysts verify the income for an adjudicated decision to determine copay status. A message then goes to VHA Enrollment System (VES) through the continuous enrollment rules engine to determine eligibility for enrollment. The results of the conversion are reported back to the Veteran's VA Medical Center treating facility. All code and algorithms are written by the VA.

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

Veterans' Health Care Eligibility Reform Act of 1996, Public Law 104-262; Title 38 U.S.C. Sections 1705, 1710, 1712 and 1722; Title 38 U.S.C Sections 5317 and 5319; Title 26 U.S.C. Section 6103 (I)(7) provide the legal authority for operating the EDB components. VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service members, reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran's benefits administered by VA.

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: EDB uses Personally Identifiable Information (PII) and Federal Tax Information (FTI). If this information were to be breached or accidentally leaked to inappropriate parties or

the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is being used in the EDB system.

Mitigation: Only information relevant to performing Means Testing and Income Verification Matching is collected. Correspondence with the Veteran may occur if additional details are needed. Only selected users have access to the information. The Department of Veterans Affairs is careful to only collect the information necessary to accomplish EDB’s mission. By only collecting the minimum necessary information, the VA is better able to protect the individual’s information.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Identification information [Name, Social Security Number (SSN), date of birth, address, phone and e-mail address]	Identification and reporting	Identification and reporting
Demographic data	Reporting	Reporting
Gender	Identification, reporting and statistics	Identification, reporting and statistics
Dependents	Identification, reporting and statistical data	Identification, reporting and statistical data
Employer information	Reporting and statistical data	Reporting and statistical data
Eligibility status	Identification, reporting and statistical data	Identification, reporting and statistical data
Enrollment status	Success/Rejection	Not used
Military service information [branch of service, discharge type and discharge date]	Reporting and statistical data	Reporting and statistical data
Veteran associates [next of kin, family members, their contact information and dependent information]	Identification, reporting and statistical data	Identification, reporting and statistical data
Financial Information [Tax Identification Number (TIN), tax returns, net income and gross income for each year Veteran enrolled]	Reporting and statistical data	Reporting and statistical data

EDB Calculation [Means test, Means test threshold amount, income year of means test]	Reporting and statistical data	Not used
--	-----------------------------------	----------

2.2 What types of tools are used to analyze data and what type of data may be produced?

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

Analysts at HEC use the EDB system to perform annual income verification of the Veteran for eligibility. HEC performs yearly Means Test on all Veterans whose eligibility is based on income. Each year analysts verify the income for an adjudicated decision to determine copay status. A message then goes to VHA Enrollment System (VES) through the continuous enrollment rules engine to determine eligibility for enrollment. The results of the conversion are reported back to the Veteran’s VA Medical Center treating facility. The EDB application produces letter correspondence to assist the analysts in gathering information from the Veteran and to inform the Veteran of any changes in their eligibility status. All code and algorithms are written by the VA.

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 annual results are reported back to the Veteran’s VA Medical Center treating facility. The EDB application produces letter correspondence to inform the Veteran of any changes in their eligibility status. VES is updated with the current analysis.

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?

Connect:Direct site-to-site VPN tunnel is used to protect data in transit intra-agency. Users communicate with the server via secure socket layer (SSL) which is encrypted with Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules approved encryption. Communications with other VA systems are over SSL, Secure Shell (SSH), Secure File Transfer Protocol (SFTP) and Techtia encryption protocols. For data at rest, all server storage arrays are protected with FIPS 140-2 approved encryption solution. Successful authentication by IVD users is required for accessing data in EDB.

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

Veteran Integrated Control Number (ICN) is used as the preferred identifier. Storage disks are running on encrypted storage arrays. Access to SSNs is only to authorized, pre-approved users. All changes to certain information are automatically logged. Data tables with special access requirements log everyone accessing the tables.

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

In order to protect veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:

1. The information with each application is categorized in accordance with Federal Information Processing Standard (FIPS) 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

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

2.4a *How is access to the PII determined?*

All VA members with access to sensitive information must complete VA Privacy and Information Security Awareness training and Sign the Rules of Behavior (ROB) as well as the Privacy and Health Insurance Portability and Accountability Act (HIPAA) training. Access to the EDB is limited to members in a valid need-to-know position and must also complete a Computer Security Agreement, Safeguarding Security Awareness and FTI training. This

training provides for the proper use and protection of sensitive information and delineates the penalties for improper use or disclosure. The System of Record Notice (SORN) defines the information collected from Veterans, use of the information and how the information is accessed and stored.

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

Audit logs are generated, monitored, and maintained to detect access anomalies. User accounts are routinely audited to determined continued access requirements. All EDB access documentation is maintained in the Light Electronic Action Framework (LEAF) system.

2.4c Does access require manager approval?

Yes

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

EDB generates audit logs of all system transactions.

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

Information System Owner (ISO) and delegates.

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

Identity information: Name, Social Security Number (SSN), date of birth, gender, address and e-mail information.

Financial information: Tax Identification Number (TIN), tax returns, and income for each year Veteran enrolled.

Military service information: branch of service, discharge type and discharge date.

Veteran associates: next of kin, family members, their contact information and dependent information.

Eligibility status, enrollment status, demographic information, dependents and employer information.

EDB Calculations: Means test, Means test threshold amount, income year of means test

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.*

Paper records are destroyed after they have been accurately scanned on optical disks. Optical disks or other electronic medium are deleted when all phases of the veteran's appeal rights have ended (ten years after the income year for which the means test verification was conducted). Data received via Connect Direct to/from SSA and the IRS are destroyed 30 days after the data has been validated as being a good copy of the original data. Summary reports and other output reports are destroyed when no longer needed for current operation. Regardless of the record medium, no records are retired to a Federal records center.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions. This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes, see Record Control Schedule (RCS) 10-1 (<https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>) Health Eligibility Center (HEC) Records, Code 1250, page 92.

3.3b Please indicate each records retention schedule, series, and disposition authority?

Per the Record Control Schedule (RCS) 10-1, Health Eligibility Center (HEC) Records, Code 1250:

1250.1; Health Eligibility Center (HEC) Records. Paper and electronic records of veterans who have applied for medical benefits at VA health care facilities, including data on the veterans' spouses. The records contain identifying information including name, address, date of birth, social security number, current eligibility category, family information, including spouse and dependent(s) name, address, social security number; employment information on veteran and spouse including occupation, employer(s) name(s) and address(es); financial information including family income, assets, expenses, debts; and third-party health plan contract information including health insurance carrier name and address, policy number and time period covered by the policy; facility location(s) where treatment is provided, type of treatment provided, i.e., inpatient or outpatient, and length of stay or number of visits. Temporary. Destroy 7 year(s) after the income year for which the means test verification was conducted, when all phases of veteran's appeal rights have ended. If an appeal is file retain records until all phases of the appeal have ended. (DAA-0015-2018-0001, item 0001)

1250.2; Tapes received from Social Security Administration (SSA) and Internal Revenue Service (IRS). Documents generated as a result of income verification by computer match with records from (IRS) and (SSA) and during the notification, verification and due process (appeals

process) periods including initial verification letters, income verification forms, income difference/final letters, confirmation/due process letters, non-response confirmation letters, clarification letters, and all subpoena documentation. Temporary. Destroy 30 days after the data has been validated as being a true copy of the original data. (DAA-0015-2018-0001, item 0002)

1250.3; Summary Reports and other output records. All forms of individual correspondence generated during the process or provided to HEC by match participants include, but is not limited to, copies of death certification; discharge certification; DD 214, notice of separation; disability award letter; IRS documents (i.e., forms 1040's W-2's, etc); State Welfare and food Stamp application; VA and other pension applicants; VA form 10-10, Application for Medical Benefits, and 10-10F, Financial Worksheet; workers compensation form; and various annual earnings statement as well as pay stubs. Temporary. Destroy when no longer needed (DAA0015-2018-0001, item 0003)

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.

Paper records are destroyed after they have been accurately scanned on optical disks. Optical disks or other electronic medium are deleted when all phases of the veteran's appeal rights have ended (ten years after the income year for which the means test verification was conducted). Data received via Connect Direct to/from SSA and the IRS are destroyed 30 days after the data has been validated as being a good copy of the original data. Summary reports and other output reports are destroyed when no longer needed for current operation. Regardless of the record medium, no records are retired to a Federal records center.

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.

PII is not used for testing, research or training for the EDB system. Federal Tax Information (FTI) does not exist outside the Production environment.

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 maintained by EDB could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, records are destroyed after they have been accurately scanned on optical disks. Optical disks or other electronic medium are deleted when all phases of the veteran's appeal rights have ended (ten years after the income year for which the means test verification was conducted). Data received via Connect Direct to/from SSA and IRS are destroyed 30 days after the data has been validated as being a good copy of the original data. Summary reports and other output reports are destroyed when no longer needed for current operation.

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
Eligibility and Enrollment - VHA Enrollment System (VES)	Means testing and Income verification matching	Name, Social Security Number (SSN), Date of Birth, Gender, Number of dependents, Eligibility Status, Enrollment Status, EDB Calculations [Means test, Means test threshold amount, and income]	Secure Socket Layer (SSL)
Health Informatics - Veterans Data Integration & Federation (VDIF)	Means testing and Income verification matching	Name, SSN, Date of Birth, Gender Internal (Z09) information: Veteran National Integrated Control Number (ICN), Veteran ICN CheckSum, bill amount, billing class, billing type, billing from date, billing To date, transaction code, transaction date, transaction type	Secure FTP (SFTP)
Health Eligibility Center (HEC) Print server	Letters to Veterans and spouse.	Letters to Veterans and spouse which may include PII and/or FTI as well as enrollment and eligibility benefits. (Name, Social Security Number (SSN), Date of Birth, Address, e-mail, Gender, Number of dependents, Eligibility Status, Enrollment Status, Tax Identification Number (TIN), tax returns, and income.)	Secure FTP (SFTP)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data within the Department of Veterans’ Affairs could happen and the data may be disclosed to individuals who

do not require access and heightens the threat of the information being misused or improperly disclosed.

Mitigation: The principle of need-to-know is strictly adhered to by EDB personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within. EDB will continue to maintain the requirement of proper credentials to communicate with these system interfaces. The system interfaces control the credentialing format and content. Access controls are in place at the wide area level through the CyberSecurity Operations Center (CSOC) gateways and firewalls. Access is further controlled by the use of Active Directory (AD) thus making only VA-approved AD users able to be added as a user of the system. Further role-based security allows users to access only that data needed to accomplish their mission. All VA employees go through privacy and security training and system administrators must complete a system administration security course.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

<i>List External Program Office or IT System information is shared/ received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/ received/ transmitted) with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
Social Security Administration	Income verification matching	Social Security Number (SSN), Name, Date of Birth, Gender, Income and Employer information	Computer Matching Agreement between SSA and VA VHA Match #1052	Connect:Direct site-to-site VPN tunnel
Internal Revenue Service	Income verification matching	Social Security Number (SSN), Taxpayer Identification Number (TIN), Name and Financial data [tax returns and income]	VHA-IRS ISA/MOU; Computer Matching Agreement between DoT IRS and VA VHA HEC	Connect:Direct site-to-site VPN tunnel

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: The privacy risk associated with sharing PII externally is that data shared outside of the Department of Veteran’s Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by EDB personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. The VA provides policy stating sharing of information will only occur if there is a contract or agreement in place. EDB has signed agreements with the IRS and the SSA. Communications to these entities are via Connect:Direct site-to-site Virtual Private Network (VPN) connections. Access controls are in place at the wide area level through the CyberSecurity Operations Center (CSOC) and VA Trusted Internet Connection (TIC) gateways and firewalls. Additionally, all data is transferred using a FIPS 140-2 compliant encryption.

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.

Public notice can be found in the System of Record Notice (SORN) “Income Verification Records-VA” 89VA10. The online “Enrollment Application for Health Benefits (VA Form 10-10EZ) includes a Privacy statement accessible from the webpage. Also, all forms requesting information from users include a Privacy notice. Those forms are:

- VA Form 10-10EZ - Application for Health Benefits
- VA Form 10-10EZR - Health Benefits Update Form
- VA Form 10-10HS - Request for Hardship Determination
- VA Form 10-301 - IRS/SSA Veteran Reported Income
- VA Form 10-302 - IRS/SSA Spouse Reported Income
- VA Form 10-302a - Spouse Additional Income Information
- VA Form 10-303 - Declaration of Representative
- VA Form 10-304 - Waiver Statement

The 10-10 forms reference the VHA Notice of Privacy Practices (NOPP) in their Privacy statements.

The VHA NOPP link is found in Appendix A-6.1 as is a copy of the Privacy Statement provided to users of the online 10-10EZ application form. Privacy notices for each VA form are

found in Appendix A-6.1 as well as the SORN link. This Privacy Impact Assessment (PIA) also serves as notice for the EDB system.

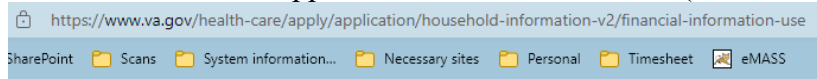
6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Copies of all Privacy statements are located in Appendix A-6.1 as well as the relevant links to the forms themselves. Also in Appendix A-6.1 is a link to the SORN “Income Verification Records-VA” 89VA10 and VHA Notice of Privacy Practices (NOPP).

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.

Each Privacy Act statement in the VA forms explains the purpose of the information collected; copies of each form’s Privacy Act Information is found in Appendix A-6.1. The online application spells out the information use before collecting Financial information.

Online “Enrollment Application for Health Benefits (VA Form 10-10EZ)



Apply for VA health care Form 10-10EZ

Step 4 of 6: Household financial information

Next we'll ask about your household financial information from 2022. We'll ask about income and expenses for you, your spouse (if you're married), and any dependents you may have.

How we use your household financial information

It's your choice whether you want to share your financial information. Before you decide, here's what to know about how we'll use your financial information.

We use your financial information to determine these factors:

- **If you're eligible for VA health care based on your income.** You may be eligible based on factors other than your income. We call these “enhanced eligibility status” factors. If you don't have one of these factors, we'll use your income to decide if you're eligible.
- **If you're eligible for travel pay reimbursement.** Reimbursement means we pay you back for the cost of travel to and from your VA health appointments.
- **If you'll need to pay a copay for non-service-connected care or prescription medicines.** This means you may need to pay a fixed amount for some types of care or medications you receive from a VA health care provider or an approved community care provider.

Note: We verify the financial information you provide with the Internal Revenue Service (IRS).

[Learn more about enhanced eligibility status for VA health care](#) ▾

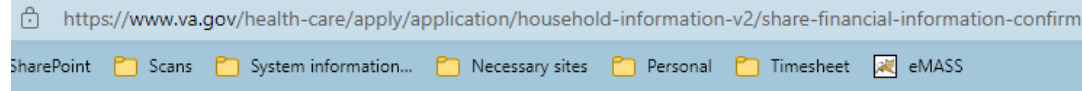
SORN “Income Verification Records-VA” 89VA10 also explains the purpose of the collected information as does this PIA.

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.

Choosing to decline to provide the requested information may lead to denial of service.

Online “Enrollment Application for Health Benefits (VA Form 10-10EZ)



Apply for VA health care Form 10-10EZ

Step 4 of 6: Household financial information

i Confirm that you don't want to provide your household financial information

If you're not eligible for VA health care based on enhanced eligibility status, we need your financial information to decide if you're eligible based on your income.

If you're eligible based on enhanced eligibility status, you don't have to share your financial information for eligibility. But if you don't share this information, we may not be able to decide if you qualify for no copays, free medications, or travel reimbursement.

« Back

Confirm »

VA Form 10-10EZ - Application for Health Benefits

Privacy Act systems of records notices and in accordance with the VHA Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA

SECTION VI - FINANCIAL DISCLOSURE

Disclosure allows VA to accurately determine whether certain Veterans will be charged copays for care and medications, their eligibility for other services and enrollment priority. Veterans are not required to disclose their financial information. Veterans who choose not to disclose financial information may not be eligible for enrollment or may be responsible for any applicable VA copayments, if they are enrolled. **Recent Combat Veterans (e.g., OEF/OIF/OND)** may answer YES in Section VI and

VA Form 10-10EZR - Health Benefits Update Form

outlined in the Privacy Act systems of records notices and in accordance with the Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA

VA Form 10-10HS - Request for Hardship Determination

systems of records notices and in accordance with the VHA Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer

VA Form 10-301 - IRS/SSA Veteran Reported Income

exception of Federal Tax Information (FTI), VA may make routine use disclosure under the authority of 45 CFR Parts 160 and 164 which permits such disclosures. The information being requested is voluntary, however failure to provide the information requested may delay or result in the denial of your health care benefits. Failure to furnish the information request will however not affect any benefits for which you are already deemed eligible due to service connection.

VA Form 10-302 - IRS/SSA Spouse Reported Income

exception of Federal Tax Information (FTI), VA may make routine use disclosure under the authority of 45 CFR Parts 160 and 164 which permits such disclosures. The information being requested is voluntary, however failure to provide the information requested may delay or result in the denial of your health care benefits. Failure to furnish the information request will however not affect any benefits for which you are already deemed eligible due to service connection.

VA Form 10-302a - Spouse Additional Income Information

of VA programs and delivery of VA benefits, verification of identity and status, and personnel administration. You do not have to provide the information to VA, but if you do not, we will be unable to process your Veteran spouse's request and serve their medical needs. Failure to furnish the information will not have any affect on any other benefits to which your Veteran spouse may be entitled. If you give VA your Social Security Number, VA will use it to administer your Veteran spouse's VA benefits, to

VA Form 10-303 - Declaration of Representative

exception of Federal Tax Information (FTI), VA may make routine use disclosure under the authority of 45 CFR Parts 160 and 164 which permits such disclosures. The information being requested is voluntary, however failure to provide the information requested may delay or result in the denial of your health care benefits. Failure to furnish the information request will however not affect any benefits for which you are already deemed eligible due to service connection.

VA Form 10-304 - Waiver Statement

acceptance of a compromise offer or for a payment plan. Disclosure is voluntary. However, if the information is not furnished, your eligibility for waiver, compromise or a payment plan may be affected. The responses you submit are confidential and protected from unauthorized disclosure by 38 U.S.C. 5701. The information may be disclosed

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.

Veterans and Service members may not decline or request that their information not be included as part of EDB's process to determine eligibility and entitlement.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Follow the format below:

Privacy Risk: There is a risk that members of the public may not know that the Enrollment Database (EDB) system exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing the System of Record Notices (SORNs), the Privacy Impact Assessment, the Privacy link from most VA websites and the Privacy Notices included on individual forms included in correspondence.

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 outlined in the System of Record Notice (SORN) "Income Verification Records-VA" 89VA10, in the Record Access Procedures, individuals seeking content of records should contact the system manager. Health Eligibility Center (HEC) Income Verification Division (IVD), the system manager noted earlier in the SORN, lists the following methods for communication: by telephone at 1 (800) 929-8387, by e-mail at VHAHECIVDMgmt@va.gov or postal service at Department of Veterans Affairs, Health Eligibility Center Income Verification Division, 2957 Clairmont Road, Suite 200 Atlanta, Georgia 30329-1647.

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)?

EDB is not exempt.

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

EDB is a Privacy Act system.

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.

As outlined in the System of Record Notice (SORN) "Income Verification Records-VA" 89VA10, in the Contesting Record Procedures, individuals seeking correction of records should contact the system manager. Health Eligibility Center (HEC) Income Verification Division (IVD), the system manager noted earlier in the SORN, lists the following methods for communication: by telephone at 1 (800) 929-8387, by e-mail at VHAHECIVDMgmt@va.gov or postal service at Department of Veterans Affairs, Health Eligibility Center Income Verification Division, 2957 Clairmont Road, Suite 200 Atlanta, Georgia 30329-1647.

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.

This Privacy Impact Assessment notifies users of the correction procedure as does the SORN “Income Verification Records-VA” 89VA10 (<https://www.federalregister.gov/documents/2023/03/23/2023-05925/privacy-act-of-1974-system-of-records>).

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.

As outlined in the System of Record Notice (SORN) “Income Verification Records-VA” 89VA10, in the Contesting Record Procedures, individuals seeking correction of records should contact the system manager. Health Eligibility Center (HEC) Income Verification Division (IVD), the system manager noted earlier in the SORN, lists the following methods for communication: by telephone at 1 (800) 929-8387, by e-mail at VHAHECIVDMgmt@va.gov or postal service at Department of Veterans Affairs, Health Eligibility Center Income Verification Division, 2957 Clairmont Road, Suite 200 Atlanta, Georgia 30329-1647.

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 the individual accidentally provides incorrect information in their correspondence.

Mitigation: Individuals provide information directly to EDB. Any validation performed would merely be the individual personally reviewing the information before he/she provides it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indication to the VA that the new information supersedes the previous data.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

The individual must be assigned to a position with an official requirement and need-to-know to gain access to the EDB. Users in the proper position with a validated background investigation must request access to the EDB through the Light Electronic Action Framework (LEAF) system. Their annual VA Privacy and Information Security Awareness training and Rules of Behavior and Privacy and HIPAA training must be current. As well, they must sign the Computer Security Agreement. The user's supervisor must approve the workflow in LEAF. The LEAF requested is routed to the EDB application administrator for the account to be created. 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 all personnel. This documentation and monitoring is performed through the use of VA's Talent Management System (TMS).

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?

No users from other agencies have access to EDB.

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.

Role-based security allows users to access only that data needed to accomplish their mission. All VA employees go through privacy and security training and system administrators must complete a system administration security course. Access controls are in place at the wide

area level through the CyberSecurity Operations Center (CSOC) gateways and firewalls. Access is further controlled by the use of Active Directory (AD) thus making only VA-approved AD users able to be added as a user of the system.

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 are prohibited from having access to the EDB Production system as part of the agreement with the IRS due to the presence of Federal Tax Information (FTI.)

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.

Annual Federal Tax Information (FTI) training is required by the IRS for those that work with FTI data. Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the 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 system. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

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

Yes

8.4a If Yes, provide:

1. *Security Plan Status:* Approved
2. *System Security Plan Status Date:* August 24, 2023
3. *Authorization Status:* Authorization to Operate (ATO)
4. *Authorization Date:* November 16, 2023
5. *Authorization Termination Date:* May 9, 2024
6. *Risk Review Completion Date:* November 9, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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**.

Not applicable to EDB.

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)

EDB does not use cloud technology.

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.

EDB does not use a Cloud Service Provider (CSP).

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.

EDB does not use a Cloud Service Provider (CSP).

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.

EDB does not use a Cloud Service Provider (CSP).

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).

EDB is not utilizing Robotic Process Automation.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

Privacy Officer, Shirley Hobson

Information Systems Security Officer, Howard Knight

Information Systems Owner, Temperance Leister


APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

System of Record Notice (SORN) “Income Verification Records-VA” 89VA10

<https://www.federalregister.gov/documents/2023/03/23/2023-05925/privacy-act-of-1974-system-of-records>

Online application (<https://www.va.gov/health-care/apply/application>) Privacy notice:

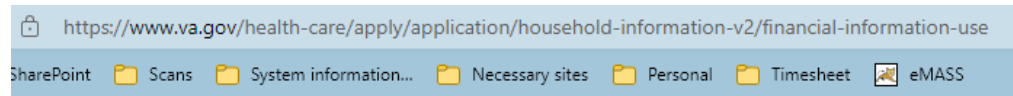


Privacy Act Statement

The Paperwork Reduction Act of 1995 requires us to notify you that this information collection is in accordance with the clearance requirements of Section 3507 of the Paperwork Reduction Act of 1995. We may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB number. We anticipate that the time expended by all individuals who must complete this form will average 30 minutes. This includes the time it will take to read instructions, gather the necessary facts and fill out the form.

Privacy Act information: VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705, 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified from initial submission forward through a computer-matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a “routine use” disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the VHA Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.

Online application form information use explanation:



Apply for VA health care Form 10-10EZ

Step 4 of 6: Household financial information

Next we'll ask about your household financial information from 2022. We'll ask about income and expenses for you, your spouse (if you're married), and any dependents you may have.

How we use your household financial information

It's your choice whether you want to share your financial information. Before you decide, here's what to know about how we'll use your financial information.

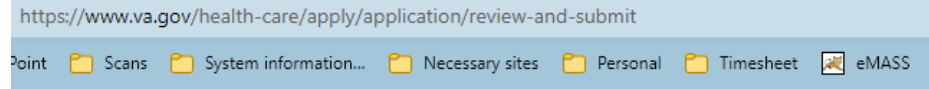
We use your financial information to determine these factors:

- **If you're eligible for VA health care based on your income.** You may be eligible based on factors other than your income. We call these "enhanced eligibility status" factors. If you don't have one of these factors, we'll use your income to decide if you're eligible.
- **If you're eligible for travel pay reimbursement.** Reimbursement means we pay you back for the cost of travel to and from your VA health appointments.
- **If you'll need to pay a copay for non-service-connected care or prescription medicines.** This means you may need to pay a fixed amount for some types of care or medications you receive from a VA health care provider or an approved community care provider.

Note: We verify the financial information you provide with the Internal Revenue Service (IRS).

[Learn more about enhanced eligibility status for VA health care](#) ▾

Online application form agreement to privacy policy (<https://www.va.gov/privacy-policy/>).



Agreement

By submitting this application, you agree to these statements:

- You'll pay any VA copays for care or services (including urgent care) that may apply, based on your priority group and other factors.
- You agree that we can contact you at the email, home phone number, and mobile phone number you gave us in the application.
- You agree to the assignment of benefits so we can bill your other health insurance or other responsible party for charges of nonservice-connected VA medical care or services.
- You've read and accept our privacy policy.

[Read our privacy policy](#)

See the VA Forms website (<https://www.va.gov/find-forms/>) for access to any of the forms below.

VA Form 10-10EZ - Application for Health Benefits

(https://www.va.gov/vaforms/medical/pdf/VA_Form_10-10EZ.pdf)

Privacy Act Information: VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705, 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified from initial submission forward through a computer-matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the VHA Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.

VA Form 10-10EZR - Health Benefits Update Form

(<https://www.va.gov/vaforms/medical/pdf/VA%20Form%2010-10EZR.pdf>)

Privacy Act Information: VA is asking you to provide the information on this form under 38 U.S.C. Sections 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified from initial submission forward through a computer matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.


VA Form 10-10HS - Request for Hardship Determination

(<https://www.va.gov/vaforms/medical/pdf/vha-10-10HS-fill.pdf>)

Privacy Act Information: VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705, 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified through a computer-matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the VHA Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.


VA Form 10-301 - IRS/SSA Veteran Reported Income
(https://www.va.gov/vaforms/medical/pdf/VA-Form_10-301.pdf)

OMB Control Number: 2900-0867
Estimated Burden: 30 minutes
Expiration Date: 06/30/2025

 Department of Veterans Affairs	IRS/SSA VETERAN REPORTED INCOME
<p>PRIVACY ACT INFORMATION: Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, 5317 and Public Law 101-508, the Omnibus Budget Reconciliation Act of 1990 grants the Department of Veterans Affairs (VA) the authority to verify Veterans' self-reported household income to determine eligibility for medical benefits. The VA also has the authority to verify Veterans' self-reported income with the Internal Revenue Service (IRS) and Social Security Administration (SSA). With the exception of Federal Tax Information (FTI), VA may make routine use disclosure under the authority of 45 CFR Parts 160 and 164 which permits such disclosures. The information being requested is voluntary, however failure to provide the information requested may delay or result in the denial of your health care benefits. Failure to furnish the information request will however not affect any benefits for which you are already deemed eligible due to service connection.</p>	


VA Form 10-302 - IRS/SSA Spouse Reported Income
(https://www.va.gov/vaforms/medical/pdf/VA-Form%20_10-302.pdf)

OMB Control Number: 2900-0867
Estimated Burden: 20 minutes
Expiration Date: 06/30/2025

 Department of Veterans Affairs	IRS/SSA SPOUSE REPORTED INCOME
<p>PRIVACY ACT INFORMATION: Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, 5317 and Public Law 101-508, the Omnibus Budget Reconciliation Act of 1990 grants the Department of Veterans Affairs (VA) the authority to verify Veterans' self-reported household income to determine eligibility for medical benefits. The VA also has the authority to verify Veterans' self-reported income with the Internal Revenue Service (IRS) and Social Security Administration (SSA). With the exception of Federal Tax Information (FTI), VA may make routine use disclosure under the authority of 45 CFR Parts 160 and 164 which permits such disclosures. The information being requested is voluntary, however failure to provide the information requested may delay or result in the denial of your health care benefits. Failure to furnish the information request will however not affect any benefits for which you are already deemed eligible due to service connection.</p>	


VA Form 10-302a - Spouse Additional Income Information
(https://www.va.gov/vaforms/medical/pdf/VA-Form_10-302a.pdf)

OMB Control Number: 2900-0867
Estimated Burden: 15 minutes
Expiration Date: 06/30/2025

 Department of Veterans Affairs	SPOUSE ADDITIONAL INCOME INFORMATION
<p>PRIVACY ACT INFORMATION: VA is asking you to provide the information on this form under Title 38, United States Code sections 1710, 1712, and 1722 in order to determine your Veteran spouse's eligibility for medical benefits. The information you supply may be verified through a computer matching program. VA may disclose the information that you put on the form as permitted by law. VA may make "routine use" disclosure for: 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. You do not have to provide the information to VA, but if you do not, we will be unable to process your Veteran spouse's request and serve their medical needs. Failure to furnish the information will not have any effect on any other benefits to which your Veteran spouse may be entitled. If you give VA your Social Security Number, VA will use it to administer your Veteran spouse's VA benefits, to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.</p>	

VA Form 10-303 - Declaration of Representative
(https://www.va.gov/vaforms/medical/pdf/VA-Form%20_10-303.pdf)

OMB Control Number: 2900-0867
Estimated Burden: 15 minutes
Expiration Date: 06/30/2025

 Department of Veterans Affairs	DECLARATION OF REPRESENTATIVE
<p>PRIVACY ACT INFORMATION: Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, 5317 and Public Law 101-508, the Omnibus Budget Reconciliation Act of 1990 grants the Department of Veterans Affairs (VA) the authority to verify Veterans' self-reported household income to determine eligibility for medical benefits. The VA also has the authority to verify Veterans' self-reported income with the Internal Revenue Service (IRS) and Social Security Administration (SSA). With the exception of Federal Tax Information (FTI), VA may make routine use disclosure under the authority of 45 CFR Parts 160 and 164 which permits such disclosures. The information being requested is voluntary, however failure to provide the information requested may delay or result in the denial of your health care benefits. Failure to furnish the information request will however not affect any benefits for which you are already deemed eligible due to service connection.</p>	

VA Form 10-304 - Waiver Statement

<https://www.va.gov/vaforms/medical/pdf/VA-Form%2010-304.pdf>

OMB Control Number: 2900-0867
Estimated Burden: 20 minutes
Expiration Date: 06/30/2025



Department of Veterans Affairs

WAIVER STATEMENT

PRIVACY ACT INFORMATION: The information you furnish on this form is almost always used to determine if you are eligible for waiver of a debt, for the acceptance of a compromise offer or for a payment plan. Disclosure is voluntary. However, if the information is not furnished, your eligibility for waiver, compromise or a payment plan may be affected. The responses you submit are confidential and protected from unauthorized disclosure by 38 U.S.C. 5701. The information may be disclosed outside the Department of Veterans Affairs (VA) only when authorized by the Privacy Act of 1974, as amended. The routine uses for which VA may disclose the information can be found in VA systems of records, including 58VA21/22, Compensation, Pension, Education and Rehabilitation Records-VA, and 88VA244, Accounts Receivable Records-VA. VA systems of records and alterations to the systems are published in the Federal Register. Any information provided by you, including your Social Security Number, may be used in computer matching programs conducted in connection with any proceeding for the collection of an amount owed by virtue of your participation in any benefit program administered by VA.

The VHA Notice of Privacy Practices (NOPP) is referenced in the VA 10-10 forms' Privacy statements. The link for VHA NOPP is

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946.

HELPFUL LINKS:

General Records Schedule

<https://www.archives.gov/records-mgmt/grs.html>

National Archives (Federal Records Management):

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

VA Publications:

<https://www.va.gov/vapubs/>

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

[VHA Notice of Privacy Practices](#)

[VHA Handbook 1605.04: Notice of Privacy Practices](#)