Privacy Impact Assessment for the VA IT System called:

Virtual VA

Veterans Benefits Administration (VBA), Compensation & Pension

Date PIA submitted for review:
March 4th, 2020

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts Table</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Rita Grewal</td>
<td><a href="mailto:Rita.Grewal@va.gov">Rita.Grewal@va.gov</a></td>
<td>202-632-7861</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Gary Dameron</td>
<td><a href="mailto:Gary.Dameron2@va.gov">Gary.Dameron2@va.gov</a></td>
<td>202-492-1441</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Arlyn De La Rosa</td>
<td><a href="mailto:Arlyn.DeLaRosa@va.gov">Arlyn.DeLaRosa@va.gov</a></td>
<td>212-807-3078</td>
</tr>
</tbody>
</table>
Abstract

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

Virtual VA provides an electronic document management system designed to improve access to claimant information.

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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes.
- Whether the completion of this PIA could potentially result in technology changes.
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?
- Does the system use cloud technology? 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.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
- 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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?
The Virtual VA (VVA) mission is to provide Compensation Service and Pension & Fiduciary Service with an electronic document management system designed to improve Veterans Service Representative (VSR) access to claimant information. This accessibility facilitates timely and accurate awards. Virtual VA is an electronic solution that reduces the need for the long-term storage and maintenance of paper-based documentation. Virtual VA moves the VA towards a paperless office by maintaining Veterans claim folders electronically rather than on paper and it centers on the concept of a Veterans electronic claims folder or eFolder.

VVA provides electronic storage for applications and evidence coming into the VA, and correspondence and ratings sent out from the VA. The system enables users to access claim information securely, quickly, concurrently with other staff, and from anywhere a user has access to the VA network. The system has the ability for a user to upload files via web interface, categorizes, search and sort the contents of an eFolder to assist in evaluating a claim and securely store and preserve the documents. It also allows users to annotate the contents of the folder with notes, and to develop lists of "bookmarks" or links to the documents, this assists in sorting the evidence by the claimant's contention or issue and it’s shared among the entire VA organization. VVA does not use cloud technology.

VVA provides the capability for batch import feeds of electronic documents from external organization such as Customer Relationship Management (CRM)/Unified Desktop (UD). VVA also receives information from internal VA sources that feed information from Debt Management Center (DMC), Department of Defense (DoD) and Defense Finance and Accounting Service (DFAS) and electronic scanning via CapturePoint for digitizing and indexing paper documents.

The eFolders systems managed by VVA are stored at three VA locations - Milwaukee, St. Paul, and Philadelphia but are accessible from any Regional Office (RO). For example, if a user needs to review information for a claim that resides in Manila, the user simply performs a search and opens the eFolder. VVA will seamlessly transfer the user to the RO where the eFolder resides, and the user will be able to review and process the claim just as easily as if the eFolder were stored in their local office.

VVA can accept claims from several sources: mail, fax, or email which will provide submission of a claim application through the Internet. Paper claims and other documents received are scanned into the system and stored into the appropriate Veteran’s eFolder. It is expected that more and more of the evidence gathered by the Veterans Benefits Administration (VBA) while processing a Veteran's claim will be available electronically. There are currently 214 million pages of information stored in the system representing 7.7 million Veterans. The system is currently used actively by 11,000 VA staff and 1,000 Veteran Service Organization (VSO) staff.

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 8111 (38 U.S.C. 58111), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C. 51104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.
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 (Enter website __________.). 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.

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother’s Maiden Name
- ☒ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Account Information
- ☐ Health Insurance Beneficiary Numbers
- ☐ Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Other Unique Identifying Number (list below)

*Zip code, Health Information

PII Mapping of Components

Virtual VA consists of one key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Virtual VA and the reasons for the collection of the PII are in the table below.
### PII Mapped to Components Table

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting PII</th>
<th>Does this function collect or store PII? (Yes/No)</th>
<th>Type of PII</th>
<th>Reason for Collection of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy Content Manager (LCM)</td>
<td>Yes</td>
<td>Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually, System Log files, sample clinical data that may contain Protected Identifiable Information (III).</td>
<td>Information contained in the images are names, SSNs, addresses, health &amp; financial info. This information is used to successfully store and mail letters to the claimant. We would need SSN/file number to successfully store the electronic version.</td>
<td>Secure File Transfer Protocol (SFTP). Up-to-date patches and encrypted channels.</td>
</tr>
</tbody>
</table>

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

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

VVA receives information from Veterans via mail, fax, or email. The SPI information is collected via electronic transmissions from Beneficiary Identification and Records Locator Subsystem (BIRLS), Corporate and Share, and batch file import (BFI) feeds.

### 1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

VVA can accept claims from several sources: mail, fax, or email. The SPI information is collected via electronic transmissions from BIRLS, Corporate and Share, and BFI feeds.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose.
This question is related to privacy control AP-2, Purpose Specification.

The Veteran information is to determine eligibility and entitlement for VA compensation and pension benefits.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Data is checked for completeness by system audits, manual verifications and annual questionnaires through automated Veteran letters. These letters ask specific questions for verification based on the existing entitlement or benefit the Veteran is receiving. The correspondence with each Veteran is then used to update the data. All collected data are matched against supporting claims documentation submitted by the Veteran. Certain data such as Social Security Number (SSN) is verified with Corporate Database (CORP). CORP verifies SSNs with the Social Security Administration for accuracy.
1.6 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

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 8111 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C. 51104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51535), titled "Agency Agreements," also known as the "Economy Act."

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: There is a risk in providing submission of a claim application through the Internet. Paper claims and other documents containing SPI, PII and or PHI received are scanned into the system and stored into the appropriate Veteran's eFolder. This could put the privacy data of individuals at risk of being inappropriately shared.

Mitigation: To reduce the risk of Veteran’s information being incorrectly shared, the following are in place.

• All employees with access to Veteran’s information are required to complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior annually.
• Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.
• Individual users are given access to Veteran’s data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user’s ID limits the access to only the information required to enable the user to complete their job.

Section 2. Uses of the Information

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

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

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

Name: Used to identify and track individual(s) in VA systems
Social Security Number: Used to identify and track individual(s) in VA systems
Date of Birth: Used to identify and track individual(s) in VA systems
Personal Mailing Address: Used to mail letters to the claimant
Zip Code: Used to mail letters to the claimant
Financial Account Information: Used to determine eligibility and entitlement for VA compensation and pension benefits.
Health Information: Used to determine eligibility and entitlement for VA compensation and pension benefits.

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

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

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

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.
Virtual VA tracks document count and insertion rates. No information pertaining to the data contained in the documents is tracked. VVA does not create or adjust the data in any way.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

- All employees with access to Veteran’s information are required to complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.
- Individual users are given access to Veteran’s data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user’s ID limits the access to only the information required to enable the user to complete their job.

**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

Virtual VA system retains the SPI information (Name, Social Security Number and Date of Birth).
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.
This question is related to privacy control DM-2, Data Retention and Disposal.

Currently the retention period on documents set to “0”, documents never gets deleted. This is because requirements were structured to adhere to the paper requirements and for Virtual VA to become of a system of record. 74 FR 29275 published June 19, 2009. [http://edocket.access.gpo.gov/2009/pdf/E9-14302.pdf](http://edocket.access.gpo.gov/2009/pdf/E9-14302.pdf)

Virtual VA (VVA) is hosted at Milwaukee and St. Paul Regional Offices and the Philadelphia Information Technology Center (PITC). The response below explains how long each data center retains information:

**PHILADELPHIA:** Regarding VVA Scanning Paper Dispositions, the Philadelphia PMC completes the following process after documents are scanned and verified in VVA/LCM/VBMS:

- If the scanned document is an original received by a claimant, the physical document is mailed back to the claimant (i.e. original copy of a DD-214, original Marriage or Death Certificate, or other types of original discharge or personal/family paperwork).

- If the document is FTI related, the physical copies are logged and maintained in secured cabinets per VBA FTI guidelines.

- All other physical paperwork is logged and prepared for shredding based on the guidelines provided under VBA 6300. Under this guidance, paperwork is recorded taken to the Regional Office Records Management Officer for proper disposal.

**ST. PAUL:** We hold the letters for 90 days after they have been verified in the system, the letters are held in a locked file cabinet then are sent to the records management officer and they are destroyed in a special shredder used only for FTI.

**MILWAUKEE:** In regard to VVA Scanning Paper Dispositions, the Milwaukee PMC completes the following process after documents are scanned and verified in VVA/LCM/VBMS:

- If the scanned document is an original received by a claimant, the physical document is mailed back to the claimant (i.e. original copy of a DD-214, original Marriage or Death Certificate, or other types of original discharge or personal/family paperwork).

- If the document is FTI related, the physical copies are logged and maintained in secured cabinets per VBA FTI guidelines (IRS Publication 1075).
• All other physical paperwork is logged and prepared for shredding based on the guidelines provided under M21-1V.iv.2.5 and VBA 6300. Under this guidance, paperwork is recorded and taken to the Regional Office Records Management Officer for proper disposal.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

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

• VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII as authorized by NARA
• Compensation, pension and Vocational Rehabilitation, Records Control Schedule VB-1 Part 1 Section XIII as authorized by NARA
• Education – Regional Processing Office, Record Control Schedule VB-1, Part 1, Section VII as authorized by NARA

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

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

Prior to destruction of any paper source documentation reclassified as duplicate copies, VA engages in a comprehensive and multi-layered quality control and validation program to ensure material that has been electronically imaged is completely and accurately uploaded into the VBMS eFolder. To guarantee the integrity and completeness of the record, VA engages in industry-best practices, using state-of-the-art equipment, random sampling, independent audit, and 100% VA review throughout the claims adjudication process. Historically, VA’s success rate in ensuring the accuracy and completeness of the electronic record routinely and consistently exceeds 99%. Furthermore, no paper document is ever destroyed while any related claim or appeal for VA benefits is still pending. VA waits 3 years after the final adjudication of any claim or appeal before destroying the paper duplicate copies that have been scanned into the VBMS eFolder. As noted, the electronic image of the paper document is retained indefinitely as a permanent record either by VA or NARA.

All other physical paperwork is logged and prepared for shredding based on the guidelines provided under VBA 6300. Under this guidance, paperwork is recorded taken to the Regional Office Records Management Officer for proper disposal.
3.5 Does the system, where feasible, use techniques to minimize the risk to privacy of 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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

VVA testing (LINKTEST) and training environments do not contain production or PII data. PII data is only housed in production databases and never populated within test. The two environments do not have a connection to each other.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

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

Follow the format below:

**Privacy Risk:** As described herein, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data on a permanent basis (beyond the actual death of the Veteran). If a master system is to be deactivated, critical information is migrated to the new system and the old system along with associated data is archived according to the application disposition worksheet. As such, SPI, PII or PHI may be held for long after the original record was required to be disposed. This extension of retention periods increases the risk that SPI may be breached or otherwise put at risk.

**Mitigation:** User access is not provided by VVA but by the ePAS process. The following are true of all VA information system users:

- All employees with access to Veteran’s information are required to complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior annually.

Version Date: February 27, 2020
Page 11 of 25
Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.

Individual users are given access to Veteran’s data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user’s ID limits the access to only the information required to enable the user to complete their job.

VVA does not create, adjust, or make documents in any way, but is simply a repository for other systems. If a document is submitted to VVA as redacted, it is input as redacted.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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.

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Database (CORP)</td>
<td>VBA would need the name/address to successfully mail a letter</td>
<td>Personally Identifiable Information (PII), Protected Health</td>
<td>Secure File Transfer Protocol (SFTP)</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>to the claimant. We would need SSN/file number to successfully store the electronic version. Depending on the letter health &amp; financial info might be contained within the letter.</td>
<td>Information (PHI), and Individually Identifiable Information (III).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>beneficiary identification and records locator subsystem (BIRLS)</td>
<td>VBA would need the name/address to successfully mail a letter to the claimant. We would need SSN/file number to successfully store the electronic version. Depending on the letter health &amp; financial info might be contained within the letter.</td>
<td>Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).</td>
<td>Secure File Transfer Protocol (SFTP)</td>
</tr>
<tr>
<td>control of veterans records system (COVRS)</td>
<td>VBA would need the name/address to successfully mail a letter to the claimant. We would need SSN/file number to successfully store the electronic version. Depending on the letter health &amp; financial info might be contained within the letter.</td>
<td>Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).</td>
<td>Secure File Transfer Protocol (SFTP)</td>
</tr>
</tbody>
</table>

### 4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:
**Privacy Risk:** There is a risk that data contained in the Virtual VA may be shared with unauthorized individuals or that those individuals, even when permit to access the data, may share it further with other individuals.

**Mitigation:**
- All employees with access to Veteran’s information are required to complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.
- Individual users are given access to Veteran’s data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user’s ID limits the access to only the information required to enable the user to complete their job.

**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: This question is #6 and #7 in the Privacy Threshold Analysis.

*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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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

N/A – The VVA project does not connect, receive, or share Personally Identifiable Information (PII) with any external (Outside of VA) organization, IT system, third-party website or application.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

**Privacy Risk:** N/A

**Mitigation:** N/A

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 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?
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. If notice was provided in the Federal Register, provide the citation.

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

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

This question is 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.

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

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

Veterans’ and their family or guardian (spouse, children, parents, grandparents, etc.) may decline or request that their information not be included to determine eligibility and entitlement for VA compensation and pension benefits. They may also choose to not designate a guardian to manage VA compensation and pension benefits. By doing so, this may impact the outcome of their claim for benefits.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

While individuals may have the ability to consent to various uses of their information at the VA, they are not required to consent to the use of their information to determine eligibility and entitlement for VA compensation and pension benefits proceeding. Once the individual has submitted all required documentation and information, the VA will determine eligibility for all VA benefits.
6.4 PRIVACY IMPACT ASSESSMENT: Notice
Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

Follow the format below:

**Privacy Risk:** There is a risk that members of the public may not know that the Virtual VA system exists within the Department of Veterans Affairs.

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

**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?**

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

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

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

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

An individual wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records, they should contact the Department of Veteran’s Affairs regional as directed in the System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA”
7.2 What are the procedures for correcting inaccurate or erroneous information?

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

An individual wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records, they should contact the Department of Veteran’s Affairs regional office as directed in the System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (July 19, 2012). This SORN can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf

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.

An individual seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1, as directed in the System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (July 19, 2012). This SORN can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf

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

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

An individual seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1, as directed in the System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (July 19, 2012). This SORN can be found online at: http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf
7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individual may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation: By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

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?

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

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and
compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed through the use of the VA’s Talent Management System (TMS).

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 or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Contractors will have access to VVA. A confidentiality agreement or a NDA are not required. OI&T provides security awareness training to all users of VA information systems or those who have access to VA sensitive information as part of initial training for new users, when required by system changes, and annually thereafter. The required course is titled VA Privacy and Information Security Awareness and Rules of Behavior (Course number VA 10176) and is available in Talent Management System (TMS). This course and the associated Rules of Behavior must be completed and acknowledged before any access is granted.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA 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 TMS. After the user’s initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through TMS.

Privacy courses in TMS are:
VA 10176: Privacy and Information Security Awareness and Rules of Behavior
VA 10203: Privacy and HIPPA Training
VA 3812493: Annual Government Ethics
8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

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

Virtual VA has been granted an Authority to Operate with Conditions (ATOC) which will expire October 7th, 2020. VVA is classified as a MODERATE system according to Federal Information Processing Standards Publication 199. VVA is consistently working towards renewal of an ATOC or full ATO. Conditions of this ATO are to ensure the system is registered with ECC’s monitoring service registry, ensure Nessus scans are conducted on a monthly bases, findings remediated, and scan results and mitigation plans are uploaded to eMASS, and Plan of Action and Milestones (POAMs) are updated; Database scan findings should be remediated, and mitigation plans uploaded to eMASS, and POAMs updated; Secure Code Review must be fully mitigated with results uploaded to eMASS and POAMs updated; Quality Code Review must be fully mitigated with results uploaded to eMASS and POAMs updated; Ensure all security documentation is up-to-date and included in eMASS; and Continued remediation of Security Control Assessment (SCA) findings.
### Section 9. References

#### Summary of Privacy Controls by Family

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

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

RITA K GREWAL
Digitally signed by RITA K GREWAL 114938
Date: 2020.09.03 17:07:07 -04'00'

Privacy Officer, Rita Grewal

Arlyn De La Rosa 130819
Digitally signed by Arlyn De La Rosa 130819
Date: 2020.08.14 12:16:24 -04'00'

Information Security Systems Officer, Arlyn De La Rosa

Gary W. Dameron 101941
Digitally signed by Gary W. Dameron 101941
Date: 2020.08.14 10:58:42 -04'00'

Information System Owner, Gary Dameron
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).

The official system of records notice (SORN), 58VA21/22/28, for “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records can be found online at:


Privacy Act Notice on VA Form 21-686c

[Image of Privacy Act Notice on VA Form 21-686c]