Privacy Impact Assessment for the VA IT System called:

Case Management System (CMS) - MicroPact Entellitrak Platform

Veterans Benefits Administration

Date PIA submitted for review:

May 12, 2020

System Contacts:

<table>
<thead>
<tr>
<th>Description</th>
<th>Name</th>
<th>E-Mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Tracy Hendrix</td>
<td><a href="mailto:tracy.hendrix@va.gov">tracy.hendrix@va.gov</a></td>
<td>202-632-7704</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Edgardo Rivera</td>
<td><a href="mailto:edgardo.rivera1@va.gov">edgardo.rivera1@va.gov</a></td>
<td>787-692-4583</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Alison Rosen</td>
<td><a href="mailto:alison.roden@va.gov">alison.roden@va.gov</a></td>
<td>202-461-9848</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.

MicroPact Entellitrak is a COTS/SaaS business solution that provides the VBA/VR&E a Case Management Solution (CMS) Service that enables Vocational Rehabilitation Counselor (VRC) engagement, data entry, benefit payments and documentation within a FedRAMP Certified cloud environment. The VR&E Solution provides benefits and assistance to approximately 950,000 eligible veterans with compensable service-connected disability (SCD) to help them obtain and maintain suitable employment or independence in living. This mission is accomplished by providing a number of direct services (e.g., comprehensive evaluation of rehabilitation needs, training and employment, independent living).

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 VA is charged with providing assistance to VR&E program participants with service-connected disabilities through VR&E services. The VR&E program is embarking on a transformative modernization which will include a suite of technological advancements to achieve the organization’s digital and paperless goals.

VR&E provides benefits and assistance to approximately 950,000 eligible veterans with compensable service-connected disabilities (SCD), service members and dependents. VR&E provides assistance (e.g., comprehensive evaluation of rehabilitation needs, training and employment, independent living) which helps claimants obtain and maintain suitable employment or independence in daily living.

The VA has authority to provide all services and assistance necessary to enable eligible Veterans with service-connected disabilities to obtain and maintain suitable employment and, if not employable, achieve independence in daily living to the maximum extent feasible. To accomplish this, the VA has a contract (#36C10E19C0004) with SBG Technology Solutions for the CMS system application. In order to facilitate the transition to the new technology, changes to VR&E business processes may occur.

The CMS application is a COTS product (Entellitrak) created by Tyler Technologies MicroPact and procured via the VR&E Business Line, which is the legal authority for this system. The CMS will be offered via a Software as a Service (SaaS) model will be hosted in a vendor-owned (non-VA) Amazon Web Services (AWS) GovCloud environment, utilizing a Virtual Private Cloud (VPC). This application instance is only used by the VA and thus is a single tenant using a FedRAMP moderate configuration. Veterans’ information will not be stored on any other contractor or sub contractor information system in order to ensure VA requirements related to data protection and media sanitization outlined in VA Handbook 6500.6 are met.

VR&E retains ownership rights to the data collected from the Veterans and from the CMS system, and is responsible for the security and privacy of the data held in the CMS system. The System of Record Notice (SORN) ID is Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records (58VA21/22/28) and is located at:


The SORN will be updated in the near future as to further align with the new CMS.

To use VR&E services, the Veteran submits an application to VR&E either online or in one of the Regional Office (RO) locations where the application is processed, and the services administered. The applications are processed by the CMS application. Subsistence allowance to the claimant is paid through the Financial Management System (FMS); other remittances to the claimants and service providers are paid through the Invoice Payment Processing System (IPPS) and FMS. CMS will allow the Vocational Rehabilitation Counselor (VRC) to manage claimants’ cases throughout the program lifecycle.
CMS provides the following functions for VR&E:

- Maintain accurate data as cases move through the vocational rehabilitation process.
- Generate VA forms and letters automatically.
- Provides a voucher processor and FMS interface to control authorizations and payments to participants.
- Provides a scheduling tool for scheduling and tracking appointments.
- Maintain a complete case history of all chronological events that have taken place in the case history.

Some of the information that will be stored in the system is:

- Name
- Mailing Address
- SSN
- E-Mail Address
- DOB
- Phone Number
- Physical Address
- School Information
- Award Data

The CMS contract states that all sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone and that the contractor shall deliver all data developed within their solution to meet all requirements of the PWS in a format that will allow VA to make use of the information. The exact format and nomenclature of this data varies, dependent on the system used, and is therefore not explicitly defined in the contract.

The VA has been granted the legal authority to operate the CMS system via Title 38, U.S.C., § 501(a) and Chapters 3, 19, 21, and 77. Title 5 U.S.C. 5514. All PII stored within the CMS will be strictly protected. Any data breach would negatively impact the VA and its mission.

All information made available to the contractor or subcontractor by the VA for the performance or administration of this contract or any information developed by the contractor or subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. Federal Acquisition Regulation (FAR) 52.227-14(d) (1) - Rights in Data - General expressly limits the contractor/subcontractor's rights to use any data acquired in the performance of this contract.

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*
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)
- Medical Record Number
- Personal Fax Number
- Personal Email Address
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Certificate/License numbers
- Other Unique Identifying Number (list below)

Additional information collected may include:

**NAME** | **USE**
---|---
Education History | To assist counselor in developing personalized rehabilitation plan.
VA Disability Rating | To determine program eligibility.
VA File Number | To identify veteran.
Entitlement History | To identify eligibility.
Dependent Information | To determine entitlement.
Handicap Status | To assist counselor in developing personalized rehabilitation plan. (Yes / No)
Service History | To determine eligibility.
Employment Status | To determine eligibility.
Employment History | To assist counselor in developing personalized rehabilitation plan.
Payment History | To determine eligibility / To update VRC with payment status.
Demographics | To identify veteran.
Emergency Contact | To provide the VRC with emergency contact information
Fiduciary Information | To determine whether the veteran has a fiduciary.
Emergency Response Indicator | To determine if the veteran is participating in any federal emergency response programs.
## PII Mapping of Components

The CMS consists of 9 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CMS and the functions that collect it are mapped below.

### PII Mapping of Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMS Application</td>
<td>Yes</td>
<td>No</td>
<td>Address, Current Medications, Date of Birth, Demographics, Dependent Information, Education History, E-Mail Address, Emergency Contact, Emergency Response Indicator, Employment History, Employment Status, Entitlement History, Fiduciary Information, Full Name, Handicap Status, IRND, Payment History, Previous Medical Records, Service History, SSN, Telephone Number, VA Disability Rating, VA File Number</td>
<td>Determine program eligibility</td>
<td>Information will be accessed by the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</td>
</tr>
<tr>
<td>CMS-DB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Version Date: February 27, 2020
Page 5 of 23
<p>| CMS Database | CRP (CorpDB) | Yes | Yes | Address Date of Birth Demographics Dependent Information Education History E-Mail Address Emergency Contact Employment History Employment Status Entitlement History Fiduciary Information Full Name Handicap Status IRND Payment History Service History SSN Telephone Number VA Disability Rating VA File Number | Determine program eligibility | Storage of this data is inside the CMS database hosted within the vendor AWS GovCloud | Storage of this data is inside the VA network / PIV card must be used to log into the VA network / Access is restricted to those users who require access and must be approved by the employee's manager / Information will be accessed by |</p>
<table>
<thead>
<tr>
<th>System Name</th>
<th>Access Rights</th>
<th>Compliant with NSOC</th>
<th>Demographics Information</th>
<th>Entitlement Processing / Eligibility Determination Information</th>
<th>VA File #</th>
<th>IRND</th>
</tr>
</thead>
<tbody>
<tr>
<td>VAEC (MPI)</td>
<td>Yes</td>
<td>Yes</td>
<td>Full Name</td>
<td>Information will be accessed by the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPI-DB</td>
<td></td>
<td></td>
<td>Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPI-DB</td>
<td></td>
<td></td>
<td>Date of Birth</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VAEC (MPI)</td>
<td>Yes</td>
<td>Yes</td>
<td>VA File #</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VAEC (MPI)</td>
<td>Yes</td>
<td>Yes</td>
<td>IRND</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS (VBMS E_FOLDER)</td>
<td>Yes</td>
<td>Yes</td>
<td>Various Letters and Forms</td>
<td>Document Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E_FOLDER-DB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS (E-VA)</td>
<td>Yes</td>
<td>Yes</td>
<td>Case ID</td>
<td>Information will be accessed by the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E_VA_DB</td>
<td></td>
<td></td>
<td>Full Name</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS (E-VA)</td>
<td>Yes</td>
<td>Yes</td>
<td>E-Mail Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E_VA_DB</td>
<td></td>
<td></td>
<td>Telephone Number</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AWS (E-VA)</td>
<td>Yes</td>
<td>Yes</td>
<td>Case Notes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E_VA_DB</td>
<td></td>
<td></td>
<td>Uploaded Documents</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VAEC (VA.GOV)</td>
<td>Yes</td>
<td>Yes</td>
<td>Full Name</td>
<td>Application Submission</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VA-DB</td>
<td></td>
<td></td>
<td>SSN</td>
<td>Information will be transmitted to</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>VA File Number</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source</td>
<td>Required</td>
<td>Provided</td>
<td>Information</td>
<td>Why Required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VA ONCE</td>
<td>Yes</td>
<td>Yes</td>
<td>Date of Birth, Address, Telephone Number, E-Mail Address, Years of Education, Future Address</td>
<td>Entitlement Processing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VA-ONCE-DB</td>
<td></td>
<td></td>
<td>Full Name, VA File Number, Entitlement History, SSN, Mailing Address</td>
<td>Information will be transmitted to and from the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VAEC - AWS (VA PROFILE)</td>
<td>Yes</td>
<td>Yes</td>
<td>Emergency Response Indicator (ERI), Fiduciary Information, Award Information, Disability Rating, Demographics, E-Mail Address, Address, Telephone Number</td>
<td>Information will be transmitted to the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VA-PRF-DB</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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.
Information in the system is provided in a variety of ways. Information can come directly from veterans, dependents, and VA Employees. Information is also provided by other VA systems such as MPI, VBMS eFolder, E-VA, and data stored within the VBA Corporate Database (CorpDB).

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.

Data is entered by the veteran into VA Form 28-1900 through automation or by VRCs who enter the data for claimants. The information on these forms is entered by the veteran or counselor onto automated screens provided by CMS and is stored in the CMS database. The form can be viewed at the following URL:


All collected information is used to determine eligibility for benefits. VBA employees may also contact a claimant directly to obtain clarifying information for benefits. Primarily, all data is entered by VRCs as part of counselor/claimant discussion.

Data is also received via integrations with other VA systems to validate claimant entitlement, usage of entitlement and manage their benefits as per the CFR and public law.

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.

All information that is collected and used in the CMS is utilized by VR&E staff to provide the necessary services and assistance to enable claimants with service connected disabilities to achieve
maximum independence in daily living and, to the maximum extent feasible, to become employable and to obtain and maintain suitable employment.

VR&E staff need to review and evaluate disabilities and other related material in order to determine entitlement to the program and collaboratively work with the claimant to develop a plan to achieve their goals and to manage their benefits payments and entitlements.

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.

Original submission of data is verified for completeness by the Regional Office staff. There are also internal program controls, edits, and checks to ensure that the data submitted is complete. Data received through the online forms are visually examined. Automated edits and audits determine that:

a. data element is present
b. value is consistent with the data requested
c. value is consistent with the record being created/updated

When feasible, data entry input through integrations with CMS are validated through a variety of common techniques, including validation against system of record details via application program integration (API). Common data validation checks include but are not limited to:

a. missing data test
b. field length test
c. class or composition test
d. reasonableness and range test
e. invalid values test
f. cross-reference tests
g. string values tests
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

PII is used internally, and shared externally, only for the authorized purposes identified in its public notices, and as authorized in System of Records Notice (SORN) 58VA21/22/28. Authority For Operation and maintenance Of The System: Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Section 501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, 55 and 77” and “Title 38, U.S.C., § 501(a) and Chapters 3, 19, 21, and 77. Title 5 U.S.C. 5514”.

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.

Privacy Risk:

Due to the highly sensitive nature of the data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached; serious personal, professional, or financial harm may result for the individuals affected.

Mitigation:
• CMS adheres to the information security requirements instituted by the VA Office of Information Technology (OIT).
• All employees with access to claimant information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
• Role based permissions will govern what participant information the data users will be able to access. The roles will be reviewed on a regular basis to ensure that appropriate information is shared with appropriate users.

Privacy Risk:

Data breach at the network level.

Mitigation:

• Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only https traffic on ports 80 and 443, along with Internet Control Message Protocol (ICMP) traffic.
• Switches ensure that the network complies with the Request for Comment (RFC) 1918 standard, and address translation technologies further enhance network security.
• IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls point of entry.

Section 2. Uses of the Information

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

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

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

The information collected from the claimant is used to determine if the claimant qualifies for benefits and the specific services to which they are entitled.

The following information is collected:
### Collected Information

<table>
<thead>
<tr>
<th>INFORMATION</th>
<th>USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>To communicate with veteran / calculate sustainment payments.</td>
</tr>
<tr>
<td>Award Information</td>
<td>To determine whether the veteran has used this benefit in the past</td>
</tr>
<tr>
<td>Bank Account Information</td>
<td>To allow veteran to verify information for sustainment payments.</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>To identify veteran.</td>
</tr>
<tr>
<td>Demographics</td>
<td>To identify veteran.</td>
</tr>
<tr>
<td>Dependent Information</td>
<td>To calculate sustainment payments.</td>
</tr>
<tr>
<td>Disability Rating</td>
<td>To assist VRC in developing personalized rehabilitation plan.</td>
</tr>
<tr>
<td>Education History</td>
<td>To assist VRC in developing personalized rehabilitation plan.</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>To communicate with veteran.</td>
</tr>
<tr>
<td>Emergency Contact</td>
<td>To provide the VRC with emergency contact information</td>
</tr>
<tr>
<td>Emergency Response Indicator</td>
<td>To determine if the veteran is participating in any federal emergency response programs.</td>
</tr>
<tr>
<td>Employment History</td>
<td>To assist VRC in developing personalized rehabilitation plan.</td>
</tr>
<tr>
<td>Employment Status</td>
<td>To assist VRC in developing personalized rehabilitation plan.</td>
</tr>
<tr>
<td>Entitlement History</td>
<td>To determine whether the veteran has used this benefit in the past</td>
</tr>
<tr>
<td>Fiduciary Information</td>
<td>To determine whether the veteran has a fiduciary.</td>
</tr>
<tr>
<td>Full Name</td>
<td>To identify veteran.</td>
</tr>
<tr>
<td>Future Address</td>
<td>To assist VRC in developing personalized rehabilitation plan.</td>
</tr>
<tr>
<td>Handicap Status</td>
<td>To assist VRC in developing personalized rehabilitation plan.</td>
</tr>
<tr>
<td>Mother's Maiden Name</td>
<td>To identify veteran.</td>
</tr>
<tr>
<td>Payment History</td>
<td>To update VRC and veteran with payment status.</td>
</tr>
<tr>
<td>Phone Number</td>
<td>To communicate with veteran.</td>
</tr>
<tr>
<td>Service History</td>
<td>To determine eligibility.</td>
</tr>
<tr>
<td>SSN</td>
<td>To identify veteran.</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>To communicate with veteran.</td>
</tr>
<tr>
<td>VA Disability Rating</td>
<td>To determine program eligibility.</td>
</tr>
<tr>
<td>VA File Number</td>
<td>To identify veteran.</td>
</tr>
<tr>
<td>Years of Education</td>
<td>To assist VRC in developing personalized rehabilitation plan.</td>
</tr>
</tbody>
</table>

#### 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
Data is checked for completeness by system audits, manual verifications, and integrations with various VA systems. Also, data is updated with each claimant correspondence. Data is updated as a result of returned mail, or returned direct deposits, or through contact with the claimant, beneficiary, or power of attorney. All data is matched against supporting claims documentation submitted by the claimant or dependents. The claimant record is manually reviewed, and data validated to ensure correct entitlement has been approved.

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.

CMS is accessed via a secured webpage utilizing SSO technology. CMS is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there.

Access to the PII is described by the System of Records Notice (SORN) for the CMS application can be found on-line at http://www.oprm.va.gov/privacy/systems_of_records.aspx.

Following is the SORN number and data:

58VA21/22/28; Name: Compensation, Pension, Education, and Rehabilitation Records-VA.

The SORN defines the information collected from veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a veteran’s benefits, such as compensation or education. The SORN will be updated in the near future as to further align with the new CMS.

CMS is implemented with the required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management
Framework for VA Information Systems. Per the approval of the Assistant Secretary for information Technology, employees such as VR&E counselors who are responding to the participants have each undergone extensive background checks and has taken the required annual privacy training, as well as signed off on Rules of Behavior document.

Access to the CMS system is requested by the employee’s supervisor and approved by the system owner. Each regional office will have assigned administrators with delegated permissions from the system owner to perform administrative functions in the system. All users will be required to authenticate to the system with a PIV card and will only have permissions to perform their assigned function. Based upon that function, each user will only have access to information on those participants which are assigned to them by their manager. The system will perform extensive logging to detail all actions taken by a user. Some of these actions are (but not limited to):

1) Logon / Logoff
2) Create Data
3) Update Data
4) Delete Data

The CMS Privacy Officer, Information System Security Officer, and Information System Owner will be responsible for maintaining all safeguards put in place to protect PII and other sensitive information.

Section 3. Retention of Information

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

3.1 What information is retained?

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

The following information is collected:

<table>
<thead>
<tr>
<th>INFORMATION</th>
<th>USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Veteran Communication</td>
</tr>
<tr>
<td>Award Information</td>
<td>Entitlement Processing</td>
</tr>
<tr>
<td>Bank Account Information</td>
<td>Entitlement Processing / Eligibility Determination</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>Entitlement Processing / Eligibility Determination</td>
</tr>
<tr>
<td>Demographics</td>
<td>Entitlement Processing / Eligibility Determination</td>
</tr>
<tr>
<td>Dependent Information</td>
<td>Entitlement Processing / Eligibility Determination</td>
</tr>
</tbody>
</table>
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.

Records management within the Department of Veterans Affairs is governed by VA Directive 6300, Records and Information Management with specific records management procedures documented in VA Handbook 6300.1. At this time, all data collected and maintained by the CMS shall be kept and/or disposed of in accordance with the VA Records Control Schedule VB-1 Section VII January 31, 2014).

For example, the following is one of many entries detailing retention mentioned in VB-1:

<table>
<thead>
<tr>
<th>Item No.</th>
<th>Title and/or Description</th>
<th>Disposition</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>07-692.020</td>
<td>Folders on eligible persons who apply for benefits but do not enter training.</td>
<td>Destroy 6 years and 3 months after expiration of eligibility delimiting date</td>
<td>NA Job NC1-15-83-13</td>
</tr>
<tr>
<td>Item No.</td>
<td>Title and/or Description</td>
<td>Disposition</td>
<td>Authority</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td>and after settlement of appeals and any other pending matters.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The document can be located at the following URL:

https://www.benefits.va.gov/WARMS/21guides.asp

During the period where data will be retained, standard operational data management capabilities will be implemented in the form of daily back-up of databases and batch data files to offline storage within the Amazon Web Services Simple Storage Service (S3), through the use of S3 Lifecycle Management rules which describe object lifecycle parameters that are created within the S3 offline storage buckets. The lifecycle configuration consists of one or more rules, where each rule defines and action for Amazon S3 to apply to one or more objects. Object lifecycle rules currently maintain offline backups with no expiration for a period of 60 days. Following 60 days, objects will be transitioned to S3 Glacier storage, which is secure, durable, and low-cost cloud storage, configured as an integral component of the e-VA application Government Cloud instance, for data archiving and long-term backup.

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.

CMS complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the CMS instance will be retained as long as the information is needed in accordance with VA Records Control Schedule VB-1 Section VII (January 31, 2014). Specific retention periods can be located in the VB-1 document at the following URL:

https://www.benefits.va.gov/WARMS/21guides.asp

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

CMS complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Participant data is never deleted in CMS. If staff “deletes” a record, a delete flag
is set which makes the record invisible, but it is never deleted. CMS backups follow a standard grandfather-father-son schema with daily incremental backups and weekly full backups on a monthly rotation. Each month’s backup is archived.

If required, the VA could export the data stored in CMS to other VA systems in order to exceed VA/NARA retention requirements. All data upon completion or termination of a contract will be turned over to VA and disposed of as soon as notice of the termination or completion is given.

When hard drives and backups are at their end of life, the media is sanitized based on GovCloud Media Disposal Policy. Hard drives are overwritten using a multiple--pass write of complementary and random values. If it wipes successfully, we will return the disk or array to the vendor. If it fails during the wiping process we retain and destroy (i.e., degauss, shred, or incinerate). Object lifecycle rules currently maintain offline backups with no expiration indefinitely. Objects may be transitioned to S3 Glacier storage, which is secure, durable, and low-cost cloud storage, configured as an integral component of the e-VA GovCloud instance, for data archiving and long-term backup.

If required, this data can be deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1.

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. 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.

CMS only uses test data (no real PII) for testing the system. VA Handbook 6500 mandates that systems under development should not process “live data” or do any real processing in which true business decisions will be based. Test data that is de-identified should be used to test systems and develop systems that have not yet undergone security A&A. Furthermore, systems that are in development (pilot, proof-of-concept, or prototype) should not be attached to VA networks without first being assessed and authorized. Additionally, VA wide Directive 6511 describes the responsibilities, requirements, and procedures for eliminating PII or information exempt from release under FOIA from presentations that may be seen by non-VA parties. This directive includes guidance for conducting privacy reviews of presentations, and the criteria for when presenters must self-certify that their presentations are devoid of PII or information exempt from release under FOIA.
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.

**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 claimant). 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:**

Redaction of some information is required by law and protects the privacy interest of any individual who may have SPI, PII, or PHI which may appear in the data and files collected.

Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. The VA procedures for eliminating data are available from the VA Records Control Schedule VB-1 (January 31, 2014). The document can be located at the following URL:

https://www.benefits.va.gov/WARMS/21guides.asp
The security controls for the CMS application cover 17 security areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems.

**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>CRP (Corporate Database / CORPDB)</td>
<td>Eligibility and entitlement determinations and service provision</td>
<td>Full Name SSN VA File Number Address Phone Number Mother's Maiden Name Disability Rating</td>
<td>Information will be transmitted to and from the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</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></td>
<td>School / Institution Information Bank Account Information Payment History Entitlement History Service History E-Mail Address Date of Birth Dependent Information Emergency Contact Information Demographics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MPI</td>
<td>Eligibility and entitlement determinations</td>
<td>Full Name Address Date of Birth VA File # IRND</td>
<td>Information will be transmitted to and from the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</td>
</tr>
<tr>
<td>VBMS EFOLDER</td>
<td>Document Storage</td>
<td>Various Letters and Forms</td>
<td>Information will be transmitted to and from the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</td>
</tr>
<tr>
<td>E-VA</td>
<td>Communication between VRC and Veteran</td>
<td>Case ID Full Name E-Mail Address Telephone Number Case Notes Uploaded Documents</td>
<td>Information will be transmitted to and from the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</td>
</tr>
<tr>
<td>VA.GOV</td>
<td>Application Submission</td>
<td>Full Name SSN VA File Number Date of Birth Address Telephone Number E-Mail Address Years of Education</td>
<td>Information will be transmitted to and from the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</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>Future Address</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VA ONCE</td>
<td>Eligibility and entitlement determinations</td>
<td>Full Name, VA File Number, Entitlement History, SSN, Mailing Address</td>
<td>Information will be transmitted to the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</td>
</tr>
<tr>
<td>VA PROFILE</td>
<td>Eligibility and entitlement determinations</td>
<td>Emergency Response Indicator (ERI), Fiduciary Information, Award Information, Disability Rating, Demographics, E-Mail Address, Address, Telephone Number</td>
<td>Information will be transmitted to the CMS system utilizing a NSOC approved Trusted Internet Connection (TIC).</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.*

**Privacy Risk:**

There is a risk that CMS data may be shared with unauthorized individual(s), or that authorized users may share it with other unauthorized individuals.

**Mitigation:**

The VA requires single sign-on (SSO) or two-factor authentication (2FA) in order to access CMS. The following security control families are applicable (in addition to all NIST applicable RMF families):

- Audit and Accountability
- Awareness Training
- Security Assessment and Authorization
- Incident Response Personnel Security
• Identification and Authentication

The CMS personnel authenticates by using PIV/passwords before accessing claimant’s information. All personnel with access to claimant’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. In addition, the following will be used to provide additional risk mitigation:

• Role-Based Access Control (RBAC) permissions for all users
• Contractor users supporting the system take all required VA 6500-specified training for their role
• Role-Based privileged user training specific to the user’s role (i.e. A system administrator must be aware of certain functions that could threaten the system’s functionality/security posture)
• CMS adheres to all information security requirements instituted by the VA Office of Information Technology (OIT)
• Information is shared in accordance with the Privacy Act, HIPAA, FOIA and VA policy

Privacy Risk:

The risk might include end users who do not log out of the CMS when away from their computers.

Mitigation:

The tool will have a definable “time-out” setting which will automatically log the user out after a period of inactivity.

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 #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

External Sharing/Receiving/Transmitting and Disclosure

<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>
</table>

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

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

- The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
- 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.
- The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for claimant PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
- 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.

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

Privacy Risk:

The privacy risk associated with maintaining PII is that sharing data outside of the VA 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 VA provides Windows and Oracle access controls along with the following security controls:

- Audit and Accountability
- Awareness Training
- Security Assessment and Authorization
- Incident Response
- Personnel Security
- Identification and Authentication.

In addition:

- All personnel with access to claimant’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- CMS adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).
- Information is shared in accordance with the Privacy Act, HIPAA, FOIA and VA policy.
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 VA provides public notice that the system does exist. This notice is provided in 2 ways:

1. The System of Record Notice (SORN):

   58VA21/22/28: SOR Name: Compensation, Pension, Education, and Rehabilitation found at:


   The SORN will be updated in the near future in order to further align with the new CMS.

2. This Privacy Impact Assessment (PIA) also serves as notice of the CMS As required by the eGovernment Act of 2002, Pub. L. 107–347 §208(b)(1)(B)(iii), the Department of claimants 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.”

In addition, individuals are given notice when applying for benefits using VA Form 28-1900, Application for Vocational Rehabilitation Benefits; Form 21-4142. Individuals will also be presented with VA Notice of Privacy Practices which contains information about data collected in the terms of use that are agreed to at registration.
6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Individuals have the right to decline providing information to VA personnel. However, failure to provide information may result in denial of VR&E Services.

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.

Individuals have the right to consent to particular uses of the information in accordance with guidelines provided in the system of records notice (SORN): VA 58VA21/22/28 (July 19, 2012). Additionally, individuals are given notice when applying for benefits using VA Form 28-1900 or VA Form 21-4142.

This SORN can be found online at:


The SORN will be updated in the near future in order to further align with the new CMS.

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.
**Privacy Risk:**

There is a risk that claimants may not understand the kind of information needed to determine entitlement to programs or to ensure the correct benefits and services are provided according to the information gathered about the claimant.

**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 this Privacy Impact Assessment and the associated System of Record Notice (SORN).

In addition, individuals are given notice when applying for benefits using VA Form 28-1900 or VA Form 21-4142.

**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.*

Individuals wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records, should contact the VA 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:
Individuals 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.

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.

Individuals wishing to obtain more information about access, redress and record correction of Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records, should contact the VA 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:


The SORN states that the procedures are the same as records access listed above. The SORN will be updated in the near future in order to further align with the new CMS.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals 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:


The SORN will be updated in the near future in order to further align with the new CMS.
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.

Formal redress procedure is provided in the SORN. Individuals 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:


The SORN will be updated in the near future in order to further align with the new CMS.

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.

Privacy Risk:

There is a risk that individuals may seek to access or redress records in the CMS 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. Furthermore, this document and the SORN provide the point of contact (POC) for members of the public who have questions or concerns about applications and evidence files. All access and redress issues are utilizing the same POC. Prior written consent or a power of attorney authorizing access is required before VA will allow the representative or attorney to have access to the claimant’s automated claims records. Contact information is listed by facility in the SORN.

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.

Contractor support teams possess privileged users responsible for maintaining the system on behalf of the VA. VA role-based security training is required for all privileged users of VA systems. Single sign-on utilizing VA PIV cards and/or Citrix VPN (over contractor laptops and unsecure networks) will be required. Typical privileged users of CMS include:

- Systems Engineer(s) - Privileged Access
- System Administrator(s) – Privileged Access
- Information System Security Engineers (Continuous Monitoring) - Auditor

The contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations. The contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (E PHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 CFR Parts 160 and 164, Subparts A and C,
the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

User roles identify the information and applications a user can access. To receive access to the system, another user with appropriate permissions must sponsor them. The sponsor will describe which applications the user needs to access, the user’s role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level control of the information and data.

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.

VA contract employee access is verified through the Contracting Officer’s Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

CMS Systems Administrators:

SBG Technology Solutions is a contractor to the VA and maintains governing authority over all CMS instances and cloud environments, where they maintain users’ hierarchies, updates environments with system-level updates and new functionality, governs deployment activity and ensures user operability. The System Administrator is not a primary user of CMS. All system administrators in SBG have signed an NDA with the VA during their on-boarding process.
8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training 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 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.

All administrative users undergo mandated annual training, including privacy and HIPAA focused training and VA privacy and information security awareness training.

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.

This document is part of the ATO submission package for CMS, which is in progress. The expected Minimally Viable Product (MVP) date is September 1, 2020.
### 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>ID</td>
<td>Privacy Controls</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</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.

Tracy M Hendrix
1466255

Privacy Officer, Tracy Hendrix

EDGARDO RIVERA-URRUTIA 116970

Information Security Systems Officer, Edgardo Rivera

Alison O Rosen
104794

Information System Owner, Alison Rosen
APPENDIX A-6.1

Notice of Privacy Practices

Effective Date: 02/14/2019

Link to VA Privacy Website: https://www.va.gov/privacy/

Privacy notice on form 28-1900:

PRIVACY ACT: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e. VA needs the information this form requests to help determine your eligibility to the benefit) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain benefits. Giving us your Social Security Number (SSN) information is mandatory. Applicants are required to provide their SSN under Title 38 USC 5101 (c) (1). The VA will not deny an individual’s benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law in effect prior to January 1, 1975, and still in effect.

Privacy notice on form 21-4142:

PRIVACY ACT NOTICE: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is voluntary. However, if the information including your Social Security Number (SSN) is not furnished completely or accurately, the source to which this authorization is addressed may not be able to identify and locate your records, and provide a copy to VA. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual’s benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975 and still in effect.
If you do not revoke this authorization, it will automatically expire in 12 months from the date you sign and date the form. Signing this form is voluntary, but failing to sign it, or revoking it before we receive necessary information could prevent an accurate or timely decision on your claim and could result in denial or loss of benefits. Although the information we obtain with this form is almost never used for any purpose other than those stated above, the information may be disclosed by VA without your consent if authorized by Federal laws such as the Privacy Act.

Under the Government Paperwork Elimination Act (GPEA) (Public Law 105-277), the Office of Management and Budget (OMB) ensures that agencies, when practicable, provide for the option of electronic maintenance, submission of disclosure of information and for the use and acceptance of electronic signatures. GPEA states that electronic records submitted or maintained in accordance with the procedures developed by OMB, or electronic signature or other forms of electronic authentication used in accordance with such procedures, "shall not be denied legal effect, validity, or enforceability merely because such records are in electronic form" (Public Law 105-277, section 1707).