Privacy Impact Assessment for the VA IT System called:

The Center for Development and Civic Engagement Portal (CDCEP)

Veterans Benefits Administration

Enterprise Program Management Office (EPMO)

Date PIA submitted for review:

09/08/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Tonya Facemire*	*Tonya.facemire@va.gov*	*202-632-8423*
Information System Security Officer	*Thomas Orler*	*Thomas.Orler@va.gov*	*708- 938-1247*
Information System Owner	*Stefano Masi*	*Stefano.Masi@va.gov*	*860- 681-9927*

Abstract

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

The Center for Development and Civic Engagement Portal (CDCEP) is an application that is used by the Department of Veterans Affairs Center for Development and Civic Engagement (CDCE), one of the largest volunteer programs in the Federal Government, to track volunteer hours and monitor membership status of the VAVS National Advisory Committee member organizations. CDCEP also tracks donations made to VA facilities nationwide. Volunteers work under Veterans Health Administration (VHA), Veterans Benefits Administration (VBA) and the National Cemetery Association (NCA) and participate in several events such as the National Veterans Wheelchair Games, National Veterans Golden Age Games, National Veterans Creative Arts Festival, and National Veterans Winter and Summer Sports Clinics. CDCEP is critical to VA in that it is used to evaluate the impact of volunteers and donations on VA's service to Veterans and provides documentation for coverage of volunteers under VA's insurance. CDCE is responsible for the strategic utilization of volunteers, donations, and community partners for the purpose of supplementing and augmenting care and services for Veterans within VHA and furthering the outreach efforts to Veterans, families and caregivers across the Department. CDCEP helps to accomplish this mission and to meet the mandatory requirements outlined in VHA Handbook 1620.01 Voluntary Service Procedures, VHA Handbook 4721 VHA General Post Fund, and VHA Handbook 1620.02 Volunteer Transportation Network.

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.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *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? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Center for Development and Civic Engagement Portal (CDCEP) application is a web application that tracks for the Department of Veterans Affairs Voluntary Service (VAVS), volunteer hours as well as donations made to VA facilities nationwide. VA volunteers work under VHA, VBA and NCA. The system is owned by Veteran Centered Experience (VCE)

CDCEP serves as the VA-wide source of tracking and compensating volunteer workers in the VA. CDCEP is used to monitor membership status of the VAVS National Advisory Committee member organizations; and provides documentation for coverage of volunteers under VA's insurance.

CDCEP streamlines Voluntary Service through better use of technology, which increases compliance with NIST-800 53 and VA 6500. By enabling VA to better serve Veterans, this effort supports the integrated objective to build our internal capacity to serve Veterans, their families, our employees, and other stakeholders efficiently and effectively.

VAVS uses CDCEP to track the thousands of volunteers used for the national rehabilitation events, such as the National Veterans Wheelchair Games, National Veterans Golden Age Games, National Veterans Creative Arts Festival, and National Veterans Winter and Summer Sports Clinics.

All volunteers (regularly scheduled and occasional) are affected: non-affiliated volunteers, members of Veterans Service Organizations, welfare, service, Veterans, fraternal, religious, civic, industrial, labor, and social groups, or clubs which voluntarily offer the services of their organizations and/or individuals to assist with the provision of care to Veteran patients, either directly or indirectly, through VA Voluntary Service under Title 38 U.S. Code § Section 513.

The information system is hosted at the Austin Information Technology Center (AITC) and is protected at the secure hosting facility which inherits procedures and policies already approved for the facility.

The mission of Center for Development and Civic Engagement Portal (CDCEP) is to provide a structured volunteer program under the management of VA compensated employees in cooperation with community resources to serve Veterans and their families with dignity and compassion. The data store by CDCEP is minimal, and is used specifically to identify VA Volunteers for two purposes: For the individual it is used to determine the overall amount of volunteer hours, in order for the VA to provide nonmonetary compensation (such as meal vouchers); in a more general sense it is used by the VA to track and report to Congress regarding Volunteer support and small donations to the VA. VAVS runs one of the largest volunteer programs in the Federal Government, supplementing staff and resources in all areas of patient care and support.

Information collected by CDCEP is not shared with other VA IT systems or Applications. It is used on the VA intranet to collect work information regarding volunteers; providing compensation as calculated internally to CDCEP; and is used to generate legally required reporting on overall volunteer activities and donations. To provide the structured volunteer program, VAVS must meet

the mandatory requirements outlined in VHA Handbook 1620.01 - Voluntary Service Procedures, VHA Handbook 4721 - VHA General Post Fund, and VHA Handbook 1620.02 - Volunteer Transportation Network.

CDCEP is accessed anywhere within the VA network via a client workstation with a VA approved Internet browser; the Applications itself is only deployed to AITC. Because the CDCEP database is only in operation at AITC, system use and PII does not vary from site to site or require more than one set of controls. CDCEP is protected at the secure hosting facility which inherits procedures and policies already approved for the facility.
Citations of the legal authority to operate CDCEP are SORN 57VA10B2A – Voluntary Service Records – VA

- Title 38 U.S. Code § Section 513
- SORN 24VA10A7 – Patient Medical Records - VA

"Voluntary Service Records-VA" (57VA10B2A) is the official identified Privacy Act Systems of Records Notice (SORN) for this PIA. However, this SORN is currently going through the official concurrence process and the SORN Number will change to 57VA10.

" Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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	☐ Mother's Maiden Name	☒ Personal Phone Number(s)
☒ Social Security Number	☒ Personal Mailing Address	
☒ Date of Birth		

☐ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers

☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☐ Integration Control Number (ICN)

☐ Military History/Service Connection
☐ Next of Kin
☐ Other Unique Identifying Information (list below)

Currently, the volunteer records consist of personal information about the individual completing an application to become a volunteer in a VA health care facility, VA regional office, or VA cemetery. Information relating to the individual membership in service organizations, qualifications, restrictions and preferences of duty and availability to schedule time of service are collected. Training records pertaining to the volunteer's service are also maintained for all active volunteers at the facility where the volunteer works, along with volunteer assignments, hours/years volunteered, and award information are retained for all volunteers. CDCEP retains the following information on its volunteers: FirstName, Last Name, Middle Name, Date of Birth, Sex, Street Address 1, StreetAddress2, City, Postal Name State, Zip Code, Telephone, Email, Address, Emergency Contact Name, and Emergency Contact Telephone.
Medical records of active volunteers are maintained in the facility's Employee Health office. Fingerprint and background investigation records are maintained by the local facility's office that handles those investigations.
The donation records require; names, address, affiliation, donation type, donation amount, donation date, donation designation, ("In Memory Of") designation, field service receipt numbers, general post fund designation, and check numbers/dates are retained for all volunteers.

PII Mapping of Components

CDCEP consists of 3 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CDCEP and the functions that collect it are mapped below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect	Does this system store	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

	PII? (Yes/No)	PII? (Yes/No)			
CDCEP CRM SaaS Azure SQL (managed by Microsoft) Cloud Base	Yes	Yes	FirstName Last Name Middle Name Date Of Birth Sex StreetAddress1 StreetAddress2 City Postal Name State Zip Code Telephone Email Address Emergency Contact Name Emergency Contact Telephone	Contacting volunteers and monitoring volunteer hours.	Managed by Microsoft as a SaaS application. No direct access is given to the Azure SQL server by Microsoft to users or customers. Access is limited to the VA's network by a link to MAG/GCC. All data access is performed through the Microsoft Dynamics CE API. This access is governed by the VA's ADO, GCC Security Groups and subsequently the CDCE Hub (Dynamics) Security Roles and Teams.
CDCEP_INTERGRATION Azure SQL Database (VA MAG)	Yes	Yes	FirstName Last Name Middle Name Date Of Birth Sex StreetAddress1 StreetAddress2 City Postal Name State	Contacting volunteers and monitoring volunteer hours.	Lives within the VA MAG on a VA owned Azure VM with SQL Server installed. All required network

			Zip Code Telephone Email Address Emergency Contact Name Emergency Contact Telephone		security settings applied, and VA network access is required to reach the server. Only the VA SQL Admins, AAD Production Service Principal, and development team admins have access. Credentials by CDCE Hub to connect to the database are stored in Azure Key Vault
VSS_OCT2021 Azure SQL Database (VA MAG)	No	Yes	FirstName Last Name Middle Name Date Of Birth Sex StreetAddress1 StreetAddress2 City Postal Name State Zip Code Telephone Email Address Emergency Contact Name Emergency Contact Telephone	Contacting volunteers and monitoring volunteer hours.	Lives within the VA MAG on a VA owned Azure VM with SQL Server installed. All required network security settings applied and VA network access is required to reach the server. Only the VA SQL Admins, and development team admins have access.

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.

Volunteers have a dedicated profile in CDCEP which includes contact information provided by volunteers to VAVS staff on the initial application (VA form 10-7055). The profile includes name, address, phone number, email, gender, emergency contact information, affiliated organization (if applicable), and volunteer assignments.

Donations are entered into a separate donation section of the CDCEP. Donors provide name, address, amount, affiliated organization (if applicable) and designation instructions for the donation. VAVS staff may record the General Post Fund (GPF) account of deposit, the check number (if made by check), an "In Memory of" designation name, and a Field Service Receipt (FSR) number. Donation data is requested by the same entities that request volunteer data and is reported in the same manner.

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 technologies 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.

Volunteer hours are collected by CDCEP after the hours are entered by the volunteers requesting daily assignments, or by VAVS staff members in the staff-facing side of CDCEP. VA form 10-7055 is used to volunteer. 10-7055 collects name, address, phone number, email, gender,

emergency contact information, affiliated organization (if applicable), and volunteer assignments; this information is provided by the volunteer.

Donors provide VAVS staff with name, address, donation amount, affiliated organization (if applicable) and designation instructions for the donation. VAVS staff may record the General Post Fund (GPF) account of deposit, the check number (if made by check), an "In Memory of" designation name, and a Field Service Receipt (FSR) number.

1.4 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.

Accuracy of data entry is assumed to be correct as it's either verbally told to a VAVS staff member directly from the volunteer or the information is written on a form by the volunteer. Volunteers can verify their information is correct when they log onto the system to check in or out at a kiosk within the VA facility at which they are volunteering.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

"Voluntary Service Records-VA" (57VA10B2A) is the official identified Privacy Act Systems of Records Notice (SORN) for this PIA. However, this SORN is currently going through the official concurrence process and the SORN Number will change to 57VA10."

Title 38 U.S. Code § Section 513
SORN 57VA10B2A – Voluntary Service Records—VA
Title 38, United States Code, Sections 501(b) and 304

SORN 24VA10A7 – Patient Medical Records - VA

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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: CDCEP collects some Personally Identifiable Information (PII) provided by volunteers. If this information were released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to those individuals.

Mitigation: VA only collects information necessary to identify the parties involved in an activity, incident, identify potential issues and concerns, and aid the affected parties in order to help parties through their crisis. By collecting minimal information, the VA better protects the information.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system 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.

Records and information collected, maintained, and disseminated by CDCEP to track the number of Regularly Volunteers, Occasional Volunteers, and student volunteers; produce statistical and managerial reports of hours and visits of all volunteers each month; and to present volunteers with certificates of appreciation for service.

The PII collected by CDCEP and its reason for usage is as follows:

- Name – Identify an Individual
- Date of Birth - Identify age and confirm identity
- Sex - Determine gender and confirm identity
- Street Address 1 - Contact the individual via mail
- Street Address 2 - Contact the individual via mail
- City - Contact the individual via mail
- Postal Name State - Contact the individual via mail
- Zip Code - Contact the individual via mail
- Telephone - Contact the individual via telephone
- Email Address - Contact the individual via email
- Emergency Contact Name - To contact if the individual has an accident and/or is injured on the job
- Emergency Contact Phone Number - To contact if the individual has an accident and/or is injured on the job

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 stored in CDCEP is not analyzed and no tools are used by CDCEP in production of information.

2.3 How is the information in the system secured?

2.3a What measures are in place to protect data in transit and at rest?

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

Information collected from Volunteers should only be used as described in this PIA. The information collected from Volunteers and validated is necessary to produce statistical and managerial reports of hours and visits of all volunteers each month.

Access to PII is determined by volunteer job categories based on management approval. The procedures for handling PII are included in the Standard Operating Procedures. Responsibility for PII is included in the Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training and signature of the Rules of Behavior. This training is mandatory on an annual basis.

The access to PII is not recorded or tracked in CRM.

2.4 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.

Add answer here:

The minimum-security requirements for CDCEP's moderate impact system cover 17 security related areas about protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include:

- access control; awareness and training; audit and accountability; assessment, authorization, and security assessments; configuration management; contingency planning; identification and authentication.
- incident response; maintenance; media protection; physical and environmental protection; planning.
- personnel security; risk assessment; systems and services acquisition; system and
- communications protection; system and information integrity.

CDCEP employs all security controls in the respective moderate impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives like the following, 6510 Identity and Access Management, 6508 Implementation of Privacy Threshold Analysis and Privacy Impact Assessment, 6403 Software Asset Management, 6309 Collections of Information, 6300 Records and Information Management, 0710 Personnel Security and Suitability Program. All personnel (employees and contractors) that work on the system complete and sign the VA Rules of Behavior.

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

Currently, the volunteer records consist of personal information about the individual completing an application to become a volunteer in a VA health care facility, VA regional office, or VA cemetery. Information relating to the individual membership in service organizations, qualifications, restrictions and preferences of duty and availability to schedule time of service are collected. Training records pertaining to the volunteer's service are also maintained for all active volunteers at the facility where the volunteer works, along with volunteer assignments, hours/years volunteered, and award information are retained for all volunteers. CDCEP retains the following information on its volunteers: FirstName, Last Name, Middle Name, Date of Birth, Sex, Street Address 1, StreetAddress2, City, Postal Name State, Zip Code, Telephone, Email, Address, Emergency Contact Name, and Emergency Contact Telephone.
Medical records of active volunteers are maintained in the facility's Employee Health office. Fingerprint and background investigation records are maintained by the local facility's office that handles those investigations.
The donation records require; names, address, affiliation, donation type, donation amount, donation date, donation designation, ("In Memory Of") designation, field service receipt numbers, general post fund designation, and check numbers/dates are retained for all volunteers.

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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.

The volunteer's record of service is maintained by the VA facility, if he or she is living and actively participating in the VAVS program.
Records are destroyed 5 years after date of last entry, final action by agency, as appropriate, but longer retention is authorized if required for business use.
Health records are stored by name and Social Security number in the patient files but are not retrievable through CDCEP.

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.

In accordance with 57VA10 – Voluntary Service Records—VA, a system of records must be maintained in Voluntary Service to include master records of Regularly Scheduled (RS) Volunteers, documents of participation of Occasional Volunteers, signed "Waiver of Claims to Remuneration Agreement," parental or guardian consent forms for student volunteers, etc. Voluntary Service administrative and general correspondence files are maintained in accordance with Records Control Schedule (RCS) 10-1 The link to the RCS is as follows: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

All volunteer records are filed by unique identification numbers within CDCEP and are cross-referenced by the organization(s) represented.

The Veterans Health Administration (VHA) Records Control Schedule (RCS) 10-1 is the main authority for retention and disposition requirements of VHA records. It provides a brief

description of the records, states the retention period and disposition requirements. It also provides the National Archives and Records Administration (NARA) disposition authorities or the General Records Schedule (GRS) authorities (as appropriate for the records). In addition to program and services sections, RCS 10-1 contains a General and Administrative (G&A) Section for records common to several offices and services. The G&A Section may be used by all VHA organizational components to dispose of their records.

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

Sensitive information downloaded or printed in hard copy format is provided the same level of security as electronic records. All paper documents and informal notations containing sensitive data are disposed of in accordance with the guidance provided at the VA Facility in which they are volunteering. Per SORN 57VA10, records are degaussed.

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

CDCEP does not use PII in its testing or pre-production environments to minimize the risk to privacy.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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: There is a risk that the information maintained by CDCEP may be retained for longer than necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risks of information retention, CDCEP adheres to NARA Records Control Schedule. When a records retention date is reached, the individuals' information is disposed off by the method described in RCS 10.1.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?
NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
N/A			

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: Maintaining PII poses the risk that data could be shared in the VA and the data may be disclosed to individuals not requiring access, increasing the risk of misused information.

Mitigation: The principle of need-to-know is strictly adhered to by CDCEP system administrators. Only personnel with a clear business purpose are allowed access to the system and the information contained.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
SSA	Social Security Administration	SSN, Name, Address	Site to Site (S2S), IPSEC Tunnel, Secure FTP	National ISA/ MOU
IRS	Internal Revenue Services	Name, Financial Information	Secure Web-Portal, Secure Socket Layer	ISA/ MOU, Computer Matching Agreement
DoD	Department of Defense	SSN, Name, Address	Bi-directional Health Information Exchange	MOU

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: PII or PHI maybe shared with unauthorized parties.

Mitigation: CDCEP has authentication and authorization processes which ensures that only authorized parties can see the data. Furthermore, there is currently no sharing of data externally.

The risks and mitigation strategies described in this section cover all the information (and information types) listed in section 1.1 of this document.

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.

Notice is provided on the application for Voluntary Service (VA 10-7055) to the individual before data collection. A copy of the form can be found at the following link: https://www.va.gov/vaforms/form_detail.asp?FormNo=7055

The following SORNs apply for CDCEP:

- 57VA10B2A: https://www.govinfo.gov/content/pkg/FR-2016-08-29/pdf/2016-20606.pdf

"Voluntary Service Records-VA" (57VA10B2A) is the official identified Privacy Act Systems of Records Notice (SORN) for this PIA. However, this SORN is currently going through the official concurrence process and the SORN Number will change to 57VA10."

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

The individual (volunteer) supplies their information via form VA 10-7555 directly to an affected end user (AEU), a VA employee, who enters the information provided by the volunteer into CDCEP. The individual has the right to decline to fill out the form, or they have the right to decline to provide the information verbally to the AEU.

The privacy notice on VA Form 10-7055 states: Disclosure of the information is voluntary, however, failure to furnish the information will hamper our ability to arrange the most satisfactory assignment for you and the Department of Veterans Affairs.

The entire paragraph from VA Form 10-7055 is as follows:
The privacy notice on VA Form 10-7055 states: The information requested on this form is solicited under the authority of 38 U.S.C. 7405(a)(1)(D) and will be used in the selection and placement of potential volunteers in the VA Voluntary Service Program. The information you supply may be disclosed outside VA as permitted by law; possible disclosures include those described in the 'routine uses' identified in the VA system of records 57VA10B2A. Voluntary Service Records-VA, published in the Federal Register in accordance with the Privacy Act of 1974. The routine uses include disclosures: in response to court subpoenas, to report apparent law violations to other Federal, State or local agencies charged with law enforcement responsibilities, to service organizations, employers and Unemployment Compensation Offices to confirm volunteer service, and to congressional offices at the request of the volunteer. Disclosure of the information is voluntary, however, failure to furnish the information will hamper our ability to arrange the most satisfactory assignment for you and the Department of Veterans Affairs.

6.3 Do individuals have the right to consent to 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

The volunteers providing their information provide their right to consent by filling out on VA Form 10-7055.

The entire paragraph from VA Form 10-7055 is as follows:
The privacy notice on VA Form 10-7055 states: The information requested on this form is solicited under the authority of 38 U.S.C. 7405(a)(1)(D) and will be used in the selection and placement of potential volunteers in the VA Voluntary Service Program. The information you supply may be disclosed outside VA as permitted by law; possible disclosures include those described in the 'routine uses' identified in the VA system of records 57VA10B2A. Voluntary Service Records-VA, published in the Federal Register in accordance with the Privacy Act of 1974. The routine uses include disclosures: in response to court subpoenas, to report apparent law violations to other Federal, State or local agencies charged with law enforcement responsibilities, to service organizations, employers and Unemployment Compensation Offices to confirm volunteer service, and to congressional offices at the request of the volunteer. Disclosure of the information is voluntary, however, failure to furnish the information will hamper our ability to arrange the most satisfactory assignment for you and the Department of Veterans Affairs.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:
Privacy Risk: The volunteer may not be aware their information can be used in response to court subpoenas, to report apparent law violations to other Federal, State or local agencies charged with

law enforcement responsibilities, to service organizations, employers and Unemployment Compensation Offices to confirm volunteer service.

Mitigation: The volunteer provides the information via VA Form 10-7055 which states: The information requested on this form is solicited under the authority of 38 U.S.C. 7405(a)(1)(D) and will be used in the selection and placement of potential volunteers in the VA Voluntary Service Program. The information you supply may be disclosed outside VA as permitted by law; possible disclosures include those described in the 'routine uses' identified in the VA system of records 57VA10B2A. Voluntary Service Records-VA, published in the Federal Register in accordance with the Privacy Act of 1974. The routine uses include disclosures: in response to court subpoenas, to report apparent law violations to other Federal, State or local agencies charged with law enforcement responsibilities, to service organizations, employers and Unemployment Compensation Offices to confirm volunteer service, and to congressional offices at the request of the volunteer. Disclosure of the information is voluntary, however, failure to furnish the information will hamper our ability to arrange the most satisfactory assignment for you and the Department of Veterans Affairs.
The individual (volunteer) supplies form VA 10-7555 directly to an affected end user (AEU), a VA employee, who enters the information provided by the volunteer into CDCEP. From that point on the volunteer is only allowed to access CDCEP via a kiosk inside a VA facility. The Volunteer Self-Service feature on the kiosk allows them to submit changes to their basic demographic information, (Name, nickname, gender, DOB), emergency contact, and their primary contact information (address, phone, email). The changes don't take effect until staff accept them in the system.

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.

Access to working areas where information is maintained in VA facilities and VA Central Office is controlled and restricted to VA employees and VA contractors on a need-to-know basis. All users of the CDCEP system are required to complete annual information system security training activities including basic security awareness training and specific information system security training provided via the Talent Management System (TMS). Members of the public are not allowed access to the CDCEP system.
Volunteers may access CDCEP via a kiosk within the VA Facility in which they are volunteering. They must use the kiosk to access CDCEP to check in to log their hours as they begin their volunteer hours. CDCEP tracks the number of hours in which they volunteer.
The volunteers are assigned a unique system assigned code and use their Date of Birth as a second factor for authentication. The kiosks have a special baseline for the set-up that locks the machine to only the CDCEP kiosk page. Volunteers don't access the full system.

An individual who wishes to determine whether a record is being maintained under his or her name in the CDCEP system or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the records are located.

The Volunteer Self-Service feature on the kiosk allows volunteers to submit changes to their basic demographic information, (Name, nickname, gender, DOB), emergency contact, and their primary contact information (address, phone, email). The changes don't take effect until staff accept them in the system.

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

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

The Volunteer Self-Service feature on the kiosk allows the volunteers to submit changes to their basic demographic information, (Name, nickname, gender, DOB), emergency contact, and their primary contact information (address, phone, email) within the CDCEP. The changes don't take effect until staff accept them in the system. Anything else that needs corrected, like time or assignments would need to be done manually, by a staff member.

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

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

Individuals are notified of the procedures for correcting their information in volunteer onboarding by each facility and the section is accessible for all volunteers as they're using the kiosk.

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 ensures data accuracy.

Individuals who desire to correct inaccurate information within CDCEP must contact their supervisor or the Chief, Voluntary Service at their facility. Staff contact VACO by emailing vhaco10b2astaff@va.gov. There are links in the system that take them to the CDCEP website where the address and contact information is listed.

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 the individual accidentally provides incorrect information in their correspondence.

Mitigation: Individuals provide information directly to CDCEP. The individual personally reviews information before providing it, as validation of the information. Individuals may provide updated information for their records by submitting new forms or indicating to the VA that new information supersedes the previous data.

Section 8. Technical Access and Security

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

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

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.

User's access to CDCEP is secured, controlled, and limited to select personnel. To gain access the user must have a VA Windows Active Directory account, and then have a CDCEP account created by either their Site Administrator at the facility or their National Administrator. The system user is then given a specific user role at the facility/facilities where access is required. Secondarily, the users must be granted access manually within the application itself. The application is designed so that users cannot gain access without:
-- being issued a user account
-- being a member of the appropriate group
-- being given access within the application itself.

All users of this system have or will have attained all required VA security approvals and documentation prior to being granted access A list of users allowed into the administrative interface is kept securely in the database. Only CDCEP Administrators have permissions to add/update/disable application users. CDCEP is made up of the following user roles:

National Administrator - Person responsible for nationwide CDCEP administration including granting all levels of user access and maintaining all national lists and reports.
National Specialist - Person responsible for assisting with nationwide CDCEP administration. Has read access to all CDCEP but write access only to National Advisory Committee and Program Manager Databases.

Site Administrator - Person responsible for site level CDCEP administration to include granting user access at their site, maintaining lists for their site, volunteer management at their site and donation tracking.
Site Specialist - Person responsible for assisting with site level CDCEP administration. Has read and write access to volunteer, timekeeping, and donation records and reports.
Site User - Person responsible for timekeeping and Donation Tracking at their site. Has read and write access to timekeeping and donation records and reports and read only access to volunteer records.
Volunteer - Person responsible for logging their own volunteer hours and printing their own meal ticket at their assigned site(s).

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

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

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

Contractors have access to CDCEP. Access is verified through VA personnel before access is granted to contractors. Contracts are reviewed annually at a minimum. Contractors providing support to CDCEP must complete annual VA Privacy and Information Security Awareness and Rules of Behavior training in TMS. All contractors are cleared using the VA background investigation 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 accessing information systems must read and acknowledge 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 the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *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.***

CDCEP is a Moderate system which is included under BAM CRM Moderate Assessing #693 – June 10, 2022 – December 7, 2022.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

The Center for Development and Civic Engagement Portal (CDCEP) is hosted on the Microsoft Azure Government Cloud (MAG) and is under Dynamics 365 VA Enterprise Contract

The Azure for Government HIGH Information as a Service (IaaS) cloud service platform is covered under the Federal Risk and Authorization Management Program (FedRAMP) P-ATO and the VA associated Cloud Service Provider (CSP) ATO documentation.

The Azure Government General Support Global Operations Services are covered under the Microsoft – Azure for Government JAB FedRAMP ATO package ID F1209051525 and the VA associated ATO.

The Microsoft Azure Government (includes Dynamics 365) SaaS Platform services are covered under the FedRAMP ATO for Microsoft Azure.

Government (includes Dynamics 365) JAB FedRAMP ATO package ID F1603087869 and the associated VA CSP-ATO.

The VA General Support Systems are covered under the VA Regions 1-6 General Support System (GSS) ATO.

The VA underlying applications are covered under their respective system owner's ATO documentation.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

VA is the owner of the data. Data rights are an explicit part of the contractual agreements (including the Business Associate Agreement) between VA and the contractor operating CRM.

Security for data stored within or processed by CRM is a responsibility shared among VA and the CRM contractor, as described at a high level. The contractor's responsibility for safeguarding the security and privacy of VA data is explicit in the contract executed between the contractor and the government. The contractor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability that can compromise the security of the systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical, but in no event longer than one calendar day.

When the security fixes involve installing third-party patches (such as patches to the Microsoft operating system or Adobe Acrobat), the contractor will, within 10 working days, provide written notice to VA that the patch has been validated as not affecting the systems. When the contractor is responsible for operations or maintenance of the systems,

they shall apply the security fixes within one calendar day. The data stored within and processed by CRM includes PHI and PII, which are information types to which VA has assigned a high-security categorization under Federal Information Processing Standard (FIPS) Publication 199 guidelines, indicating the potential for high impact if such data is disclosed to unauthorized parties.

The Azure for Government HIGH Information as a Service (IaaS) cloud service platform is covered under the Federal Risk and Authorization Management Program (FedRAMP) P-ATO and the VA associated Cloud Service Provider (CSP) ATO documentation.

The Azure Government General Support Global Operations Services are covered under the Microsoft – Azure for Government JAB FedRAMP ATO package ID F1209051525 and the VA associated ATO.

The Microsoft Azure Government (includes Dynamics 365) SaaS Platform services are covered under the FedRAMP ATO for Microsoft Azure.

Government (includes Dynamics 365) JAB FedRAMP ATO package ID F1603087869 and the associated VA CSP-ATO.

The VA General Support Systems are covered under the VA Regions 1-6 General Support System (GSS) ATO.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

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

Yes, for all cloud deployments the VA own data and identities.

The following responsibilities are retained and accountable for security and privacy by the organization:

- Data
- Endpoints
- Accounts
- Access management

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2022.09.30 13:11:27 -04'00'

Privacy Officer, Tonya Facemire

Thomas J. Orler 178546

Digitally signed by Thomas J. Orler 178546
Date: 2022.09.30 12:23:44 -05'00'

Information Systems Security Officer, Thomas Orler

Stefano Masi 474380

Digitally signed by Stefano Masi 474380
Date: 2022.10.03 16:19:34 -04'00'

Information Systems Owner, Stefano Masi

APPENDIX A-6.1

Notice is provided on the application for Voluntary Service (VA 10-7055) to the individual before data collection. A copy of the form can be found at the following link: https://www.va.gov/vaforms/form_detail.asp?FormNo=7055

The following SORNs apply for CDCEP:

- 57VA10B2A: https://www.govinfo.gov/content/pkg/FR-2016-08-29/pdf/2016-20606.pdf

"Voluntary Service Records-VA" (57VA10B2A) is the official identified Privacy Act Systems of Records Notice (SORN) for this PIA. However, this SORN is currently going through the official concurrence process and the SORN Number will change to 57VA10."