Privacy Impact Assessment for the VA IT System called:

National Caregiver Training Portal

Veterans Health Administration

CAREGIVER SUPPORT PROGRAM (12CSP)

eMASS ID #2506

Date PIA submitted for review:

September 10, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	Dennis.Lahl@va.gov	202-461-7330
Information System Security Officer (ISSO)	Amine Messaoudi	Amine.Messaoudi@va.gov	202-815-9345
Information System Owner	Kandace Smith	Kandace.Smith@va.gov	215-834-2519

Abstract

The National Caregiver Training Portal is a secure referral website that allows caregiver support staff to make referrals containing caregiver Personal Identifiable Information (PII) such as name of caregiver, personal mailing address, personal phone number, personal email address, and Caregiver Record Management Application ID (CARMA ID). This referral website will allow verification of eligibility prior to participation. Through this verification process, the Contractor (CoreTech Global) ensure all participants are verified as eligible for the corresponding training through confirmation from the local caregiver support program staff via participant name and CARMA ID number corresponding to the primary and secondary caregivers.

This portal is specifically tailored to support the case management needs of VA Caregiver Support Program (CSP) staff for the National Caregiver Training Program. Over 1700 VA CSP staff rely on this portal to submit new referrals for training certification and manage the training history for thousands of VA caregivers which is a requirement in order to be approved for either the Program of Comprehensive Assistance for Family Caregivers (PCAFC) or the Program of General Support Services (PGCSS).

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?
National Caregiver Training Portal - Caregiver Support Program Office (12CSP)

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

The Caregivers and Veterans Omnibus Health Services Act of 2010 (P.L 111-163) established 38 U.S.C. 1720G, directed the Department of Veterans Affairs (VA) to establish a Program of Comprehensive Assistance for Family Caregivers (PCAFC) and a Program of General Caregiver Support Services (PGCSS). Both programs are managed by the VA's Caregiver Support Program (CSP) Office. On June 06, 2018, the President signed into law the VA Maintaining Systems and Strengthening Integrated Outside Networks (MISSION) Act of 2018 or the VA MISSION Act of 2018 (P.L. 115-182). The VA MISSION Act of 2018 fundamentally transformed elements of the Department of Veteran Affairs' (VA) healthcare system to include expansion of the PCAFC within the CSP (38 U.S.C. 1720G; 38 CFR Part 71). The CSP must implement changes required by section 161 of the VA MISSION Act of 2018, improve PCAFC, and to ensure consistency in how PCAFC is administered across VA.

Under the PCAFC, Caregivers are eligible for a host of the Department of Veterans Affairs (VA) services including services a monthly stipend, access to CHAMPVA (if eligible), mental health counseling, caregiver training, enhanced respite services, certain beneficiary travel, and ongoing monitoring. One of

the requirements to participate in this program is the completion of the National Caregiver Training. The NCTP provides this training through web-based online training with CD/DVD for reference. These training modalities must be offered in English and Spanish.

C. Who is the owner or control of the IT system or project?
CoreTech Global

2. Information Collection and Sharing

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

As of 08/01/2024, there were 82,352 caregivers that completed training. The caregiver is a spouse, family member or paid helper that takes care of our Veterans.

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

The data elements in the system are:

Name of caregiver
Personal mailing address
Personal phone number
Personal email address
CARMA ID - Caregiver Records Management Application (CARMA) is a unique identification number generated by Salesforce which is used to track Veteran/caregiver interactions, such as calls, referrals, applications, and reassessment processes in relation to the Caregiver Support Program.

The purpose for collecting this information is track the following:

Number of participants referred (including a breakdown of referrals by individual CSP teams and their VAMC location
Completion rates
Demographics of caregiver participation
Number of caregivers completions status who have initiated training broken down by:
Hardcopy (Workbook)
Web-Based
Large Print
Training by Language
Completion rates
Trending data

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

The following data elements is shared with the Caregiver Support Program Staff

Name of caregiver
Personal mailing address
Personal phone number
Personal email address
CARMA ID

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

The system is only operated in one site.

3. Legal Authority and SORN

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

The Privacy Act of 1974, as amended, 5 U.S.C. 552a, establishes a code of fair information practices that governs the collection, maintenance, use and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1. falls under Title 28, United States Code, title 38, U.S.C., sections 501 (a), 1705, 1710, 1722, and 5317.

https://www.oprm.va.gov/privacy/systems_of_records.aspx .

197VA10 / 89 FR 6568 - Caregiver Support Program—Caregiver Record Management Application (CARMA)—VA - https://www.govinfo.gov/content/pkg/FR-2024-02-01/pdf/2024-01984.pd

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

No.

4. System Changes

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

No

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

No.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

✓ **Name**
☐ Social Security Number
☐ Date of Birth
☐ Mother's Maiden Name
✓**Personal Mailing Address**
✓**Personal Phone Number(s)**
☐ Personal Fax Number
✓**Personal Email Address**
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers
Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
✓ Other Data Elements
VA Email Address
VA Phone Number
Contractor email address
Contractor name
CARMA ID

PII Mapping of Components (Servers/Database)

The National Caregiver Training Portal (NCTP) consists of one key component SQL Database. This component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by NCTP and the reasons for the collection of the PII are in the table below.

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

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
SQL Database	Yes	Yes	Name Personal Mailing address Personal Phone number Personal email address CARMA ID	Collection and storage needed to register and track new caregivers for the mandatory training	**Role-Based Access Control (RBAC):** Access to sensitive data is restricted based on user roles, ensuring that only authorized personnel can access PII. **Data Minimization:** We collect and retain only the minimum necessary PII to serve the system's purpose, minimizing risk exposure. **Encryption:** All data is encrypted at rest using TDE (Transparent Data Encryption). All data is also encrypted in transit as TSL (Transport Layer Security) 1.2 is required for all connections to the database. **SQL Injection Prevention:** Parameterized queries and input validation prevents SQL injection attacks that can compromise the database. **Encrypted Backups:** Database backups are encrypted to prevent unauthorized access to data in case of a breach or physical theft.

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Caregivers that are deemed eligible for PCAFC services by our Centralized Eligibility Appeals Team, the Caregiver Support Coordinator (CSC) submits the referral into the NCTP.

The CSC enters the caregiver information (name, email address, mailing address, phone number and CARMA ID into the portal.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

The application/approval process for caregiver support services is managed by the Caregiver Support Program Office. The program office utilizes the CARMA ID to confirm the eligibility of all caregivers. The Caregiver Records Management Application (CARMA) provides a comprehensive and integrated approach to caregiver record management by streamlining processes and improving reporting capability. It is built on Salesforce.com, a robust and user-friendly Software as a Service (SaaS) platform. CARMA tracks and manages Veterans, Contacts, Facilities, Applications, Caregivers, Appeals, Calls and Referral data.

CARMA is a module built on the Salesforce platform to support Family Caregivers of Veterans. Under section 101 of Public Law (PL) 111-163, designated primary Family Caregivers of eligible Veterans participating in the Program of Comprehensive Assistance for Family Caregivers may be eligible to receive a monthly stipend, access to health record used to track interactions, such as calls, referrals, applications, and re-assessment processes with/for a person in relation to the CARMA program coverage through CHAMPVA, education & training, respite care, mental health care and travel benefits when they accompany a Veteran for care or attend required training. CARMA is designed to assist in meeting the business requirements of the Caregiver Support Program Overview.

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

The system creates the following reports:

Monthly completion dates
Completions without a certificate
Export raw data of Caregivers (number of Caregivers in the portal)
Export raw data of Caregiver Support Coordinators (VA Staff) in the portal
Export raw data of training assignments in the portal
Languages requested (beyond English/Spanish)

1.3 How is the information collected?

Caregiver Support Coordinators (CSCs) collect required user information from the Caregivers PCAFC applications and at times directly from the caregiver. The CSC directly input data into the NCTP Referral Portal via individual, authenticated CSC accounts.

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

During the application process, the Caregiver Support Coordinator (VA staff) contact the caregiver to collect/confirm the information directly from the individual.

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

Federal Register :: Program of Comprehensive Assistance for Family Caregivers Improvements and Amendments Under the VA MISSION Act of 2018 The instructions and application to apply for PCAFC can be found:

Program of Comprehensive Assistance for Family Caregivers (PCAFC) - VA Caregiver Support Program

Caregiver Application For Benefits | Veterans Affairs (va.gov)

This form is used to apply for VA's Program of Comprehensive Assistance for Family Caregivers (PCAFC). VA will use the information on this form to assist in determining your eligibility. A Veteran, as defined herein, may appoint one (1) Primary Family Caregiver applicant and up to two (2) Secondary Family Caregiver applicants. On average, it will take 15 minutes to complete the application, including the time it will take you to read the instructions, gather the necessary facts and fill out the form. Each time a new Primary or Secondary Family Caregiver is requested, a new Form 10-10CG is required. This includes a caregiver who is already approved and designated as a Primary Family Caregiver and wishes to be designated as a Secondary Family Caregiver, or a caregiver who is already approved and designated as a Secondary Family Caregiver who wishes to apply as a Primary Family Caregiver.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that

receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The system does not use a process to check the data. Data is validated at each chain of custody within the VA as it moves through processes we use the data. There are multiple peer reviews at each level**.**

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

No.

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

Title I of Public Law 111-163, Caregivers and Veterans Omnibus Health Services Act of 2010 (hereinafter referred to as "the Caregivers Act"), established section 1720G(a) of title 38 of the United States Code (U.S.C.), which required VA to establish a program of comprehensive assistance for Family Caregivers of eligible veterans who have a serious injury incurred or aggravated in the line of duty on or after September 11, 2001. The Caregivers Act also required VA to establish a program of general caregiver support services, pursuant to 38 U.S.C. 1720G(b), which is available to caregivers of covered veterans of all eras of military service. VA implemented the program of comprehensive assistance for Family Caregivers (PCAFC) and the program of general caregiver support services (PGCSS) through its regulations in part 71 of title 38 of the Code of Federal Regulations (CFR). Through PCAFC, VA provides Family Caregivers of eligible veterans (as those terms are defined in 38 CFR 71.15) certain benefits, such as training, respite care, counseling, technical support, beneficiary travel (to attend required caregiver training and for an eligible veteran's medical appointments), a monthly stipend payment, and access to health care (if qualified) through the Civilian Health and Medical Program of the Department of Veterans Affairs (CHAMPVA). 38 U.S.C. 1720G(a)(3), 38 CFR 71.40.

1.6 PRIVACY IMPACT ASSESSMENT:

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete this section)

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Yes. Each application refers to Federal Laws (18 U.S.C. 287 and 1001) and requires a signature from the caregiver.

Federal Laws (18 U.S.C. 287 and 1001)provide for criminal penalties for knowingly submitting false, fictitious or fraudulent statements or claims. I certify that I am at least 18 years of age. I certify that either: (1) I am a member of the Veteran's family (including a parent, spouse, a son or daughter, a step-family member, or an extended family member) OR (2) I am not a member of the Veteran's family, and I reside with the Veteran full-time or will do so upon designation as the Veteran's Primary Family Caregiver. I attest that my application and/or participation in PCAFC is as the Veteran's Family Caregiver. I acknowledge my eligibility for any payment and/or other benefit that results is contingent on the Veteran's eligibility and participation and as such the Veteran is involved in my payment related activities. I agree to perform personal care services as the Primary Family Caregiver for the Veteran named on this application. I understand that the Veteran or the Veteran's surrogate may request my discharge from the Program of Comprehensive Assistance for Family Caregivers (PCAFC) at any time and that my designation as a Primary Family Caregiver may be revoked or I may be discharged from PCAFC by the Secretary of Veterans Affairs (or designee) as set forth in 38 CFR 71.45. I understand that participation in the PCAFC does not create an employment relationship between me and the Department of Veterans Affairs. I certify that the information provided in this form is correct and true to the best of my knowledge and belief.

Follow the format below when entering your risk assessment:

Privacy Risk: The privacy risk in the collection of the data elements (personal contact information) in the verification of eligibility into the CSP program could happen and data may be disclosed to those who do not do not require access and heightens the threat of the information being misused..

Mitigation: To mitigate this risk, the principle of need–to–know is strictly adhered to by the Caregiver Support Program personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within. Access control for CoreTech is accomplished through VA Contract Officer Representative confirming completion of background

check and TMS trainings. Access control for VA staff is accomplished through portal access requests via active VA email address and confirmation of Caregiver Support Coordinator assignment within the facility.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name of Caregiver	File Identification purposes	Not used
Caregiver Mailing Address	File Identification purposes	Not used
Caregiver Personal Phone Number	File Identification purposes	Not used
Caregiver Email Address	File Identification purposes	Not used
CARMA ID	File Identification purposes	Not used
VA Email Address	File Identification purposes	Not used
VA Phone Number	File Identification purposes	Not used
Contractor email address	File Identification purposes	Not used
Contractor name	File Identification purposes	Not used

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

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

Data dashboards, charts, and reports (as listed in 1.2c) are created through Microsoft Power BI.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the

individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The system does not inherently "create" new or previously unutilized information about an individual. Any new information is manually entered and updated by the VA staff or CoreTech staff. All requests to update information are initiated either through Portal system communication channels, email to Caregivertraining@technologywerks.com, or via phone. Such information could include a change in shipping or email address, name, or training modality. All updated information is applied to the original individual record, and all updated information is accessible to CoreTech program support specialists and to Caregiver Support Coordinators (CSCs) aka Government employees who make determinations about the individual.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Data in transit from the database is protected through secure SSL and HTTPS protocols to the application.

Data at rest in the database is protected through TDE (Transparent Data Encryption).

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

Social Security Numbers are not collected.

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

We conduct a thorough inventory to determine the PII that is collected, collect only the data necessary to complete the project, and employ security controls such as encryption and access controls.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Portal access for CoreTech Program Support Specialists is determined by the VA COR after user successfully completes TMS training and background check. Portal access for Caregiver Support Coordinators (VA staff) is initiated through the "Register New Account" button. CSCs are then prompted to enter their information including active VA email address which must align with the correct VISN and Facility. A message is then sent to their VA email where they are prompted to "Confirm Account" and set a password.

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

For CoreTech Program Support Specialists – training certificates are documented yearly.

2.4c Does access require manager approval?

Yes. CoreTech provides internal training on Portal navigation and NCTP support protocols. This is done primarily through multiple one-on-one training sessions and additionally through job shadowing. CoreTech staff are then granted access to the Portal once VA requirements and internal training has been completed (1-2 week process).

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

Access to the PII is equivalent to access to the Portal. Portal access (and PII access) is strictly limited to active CSCs and credentialed CoreTech staff. those with active Portal access. Access to all Portal information is monitored via a log which records the activity time/date stamp and identity of every Portal login. Once a CoreTech staff members is no longer serving on the NCTP contract, their access is immediately removed by CoreTech. Once CSCs are no longer serving in that capacity, the lead Coordinator requests via email the removal of the CSC from the Portal, effectively removing their access.

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

Sam Goldgeier is our CoreTech Portal Developer who is responsible for assuring safeguards for the PII.

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

Name of caregiver, personal mailing address, personal phone number, personal email address and CARMA ID

3.2 How long is information retained?

Retention of Records is expected to be 75 years. The information is retained following the policies and schedules of VA's Records Management Service and National Archive and Record Administration (NARA) in "Department of Veterans Affairs Records Control Schedule 10-1". Record Control Schedule 10-1 can be found at the following link:
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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

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

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

NCTP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the NCTP will be retained as long as the information is needed in accordance with a NARA-approved retention period.

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

Yes. The Records Control Schedule (RCS) 10-1 provides VHA records retention and disposition requirements for VHA Central Office, Program Offices, and field facilities. The VHA Records Control Schedule (RCS) 10-1 is the main authority for the retention and disposition requirements of VHA records. It provides a brief description of the records and states the retention period and disposition requirements. VHA RCS 10-1, dated January 2019

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

The retention schedule is under Item Number 7900 – The Caregiver Record Management Application (CARMA).
Disposition Instructions – Temporary – Destroy 75 years after enrollment
Disposition Authority – DAA-0015-2020-0001-0001

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

All data stays in the NCTP until the VA initiates process for deletion. A certificate of destruction is issued once the media is physically destroyed. Electronic data and files of any type, including PII are destroyed in accordance with the Department of Veterans' Affairs VA Directive 6500 (January 24, 2019), https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf).

Per the contract - Any data destruction done on behalf of VA by a contractor/subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization

For instances when workbooks are mailed to caregivers, CoreTech disposes paperwork/shipping envelopes that contain caregiver PII by using a shredding service called called Shred-it approximately every three months. Shred-it uses a systematic and secure process to ensure confidential information is properly shredded and disposed of.

1. **Collection**: Shred-it provides secure containers (locked bins or consoles) to clients for collecting confidential documents. These containers are designed to prevent unauthorized access. Employees of the client place sensitive documents directly into these containers without handling them further.
2. **Scheduled Pickup**: Shred-it's trained and vetted service representatives visit the client's site on a scheduled basis to collect the contents of the secure containers. They ensure the documents remain locked and secure during transport.
3. **On-site or Off-site Shredding**:
    - **On-site shredding**: Shred-it has mobile shredding trucks equipped with industrial shredders. The service representative brings the locked containers to the truck, where the documents are shredded on-site in the client's presence, offering real-time assurance of secure destruction.
    - **Off-site shredding**: Alternatively, the documents may be securely transported to a Shred-it facility where they are shredded under strict security protocols.

4. **Shredding Process**: Once the documents reach the shredder, whether on-site or at a facility, they are processed through industrial-grade shredders that cut the paper into small, unrecognizable pieces. This makes reconstruction of documents virtually impossible.
5. **Recycling**: After shredding, the shredded material is baled and sent to recycling plants where it is processed into new paper products. This step ensures environmental responsibility by reducing waste.
6. **Certificate of Destruction**: After the shredding is complete, Shred-it provides the client with a Certificate of Destruction. This document confirms that the materials were securely destroyed according to industry standards and can be used for audit or compliance purposes.

Shred-it's process complies with privacy laws and regulations such as HIPAA, FACTA, and GDPR, ensuring the secure handling and destruction of sensitive information.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

The Caregiver Support Program Office does not use PII for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT:

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged? No.
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: The risk to maintaining data within the NCTP is that longer retention times increase the risk that information can be compromised or breached.

Mitigation: The principle of need–to–know is strictly adhered to by the Caregiver Support Program personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within. Access control for CoreTech is accomplished through VA Contract Officer Representative confirming completion of background check and TMS trainings. Access control for VA staff is accomplished through portal access requests via active VA email address and confirmation of Caregiver Support Coordinator assignment within the facility

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?

We do not share information. Information that has to be validated (Caregiver contact information-phone/email) is sent to Caregiver Support Coordinators thru the portal or thru encrypted email

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.

Information is not shared. If data validation is needed, the contractor will contact the Caregiver Support Staff.

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

Information is not shared.

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.

Information is not shared. If data validation (email and shipping/home address) is needed, the contractor will reach out to the Caregiver Support Coordinator (VA staff) thru the NCTP

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
Caregiver Support Program	Information is not shared. Information for data validation is sent thru the messaging center in the NCTP to the VA staff work email address	Name Personal Mailing Address Personal Phone Number Personal Email Address VA Email Address CARMA ID	Messages thru email

Information is not shared. Information for data validation is sent thru the messaging center in the NCTP to the VA staff work email address.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The NCTP privacy risk associated with maintaining PII within the Department of Veterans' Affairs could happen and that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: We do not share internally.

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.

There is no sharing/receiving with external organizations.

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
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: No external sharing

Mitigation: No external sharing

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Yes.

For the online application there is a link to View Privacy Act Statement on the page before the Veteran or Caregiver can begin the application. Also on the last page of the online application before submission, the Veterans's Statement of Truth includes the following statement:

I have read and accept the privacy policy (hyperlink must be clicked on). The link for privacy policy takes the applicant to the VA.Gov – Privacy, policies and legal information site (see Appendix A-6.1). The name of the applicant must be entered into the field along with the certification that the information provided is correct and true.

For the paper application, the Privacy Act Information is listed on page 2 of the Please Read Before you Start instruction sheet.

6.1b If notice was not provided, explain why.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

VA is asking you to provide the information on this form under 38 U.S.C. Sections 101, 5303A, 1705, 1710, 1720B, 1720G, 1725 and 1781 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified through a computer-matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records, “Patient Medical Records --VA” (24VA10A7), “Enrollment and Eligibility Records --VA” (147VA10), and “Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA” (54VA10NB3), Caregiver Support Program - Caregiver Record Management Application (CARMA) - VA (197VA10) and in accordance with the VHA Notice of Privacy Practices. Records in CARMA are used to administer, monitor and track services and benefits sought and delivered through VA's Caregiver Support Program. Veteran and Family Caregiver Applicants each have their own individual records within CARMA. Providing the requested information, including Social Security Number, is voluntary, but if any requested information is not provided, it may delay or result in denial of the request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits, and their records, and for other purposes authorized or required by law.

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 information however incomplete fields may result in delay or denial of PCAFC benefits.

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

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.

Yes VHA Handbook 1605.01 'Privacy and Release Information', Section 5 a. (6) lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually-identifiable health information to carry out treatment, payment, or health care operations. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record.

6.4 PRIVACY IMPACT ASSESSMENT:

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

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

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

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

Privacy Risk: There is a risk that VA employees and Veterans/Caregivers will not know that NCTP collect, maintains, and/or disseminates Personally Identifiable Information (PII) about them.

Mitigation: The Caregiver Support Program mitigates this risk by ensuring that it provides individuals notice of information collection through the methods discussed in question 6.1. The VA mitigates this risk by allowing only personnel with a clear business purpose are allowed access to the system and information contained within.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions**. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.**

Caregivers may access their information thru the agency's Freedom of Information Act (FOIA) (5 U.S.C 552) enacted to give individuals the right to access information from the federal government and sets a government-wide standard for the disclosure or withholding of records. FOIA provides judicial remedies, as needed, to those who think that they have been wrongfully denied access. A Veteran and/or caregiver can submit a written, signed and reasonably described request seeking records from the Caregiver Support Program Office.

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

Our system – application/online form is not exempt from the Privacy Act

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

Our system – application/online form is not exempt from the Privacy Act

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 Veteran is responsible for entering in the accurate data on their application. This information is collected for the purposes of initiating the mandatory training needed to participate in the CSP program. The information from the application is entered into the NCTP by Caregiver Support Coordinators (CSC). CoreTech staff will reach out to the Caregiver Support Coordinators to report inaccurate information. The CSC (VA Staff) will research and update the inaccurate information in the NCTP.

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.

Bi-annual CSP Staff NCTP Education Call, immediate and direct communication via email thru the NCTP Portal.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. **Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.**
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Caregivers do not have access to the NCTP. If redress is needed they will contact their Caregiver Support Coordinator or thru FOIA.

7.5 PRIVACY IMPACT ASSESSMENT:

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

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:

Privacy Risk: There is a risk that Veterans/caregivers information is incorrect and may not receive the mandatory training workbook/online training in a timely manner. Furthermore, incorrect information may result in delay of receiving CSP benefits.

Mitigation: NCPT mitigates the risk of incorrect information in an individual's records by authenticating information and validating data accuracy using the procedures discussed in question 7.2.
There is a message center linked to each caregiver account (communication log) that will send the message to their Caregiver Support Coordinator.

Section 8. Technical Access and Security

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

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

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

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

Caregiver Support Coordinators access the system through "Register New Account" button. CSCs are then prompted to enter their information including active VA email address which must align with the correct VISN and Facility. A message is then sent to their VA email where they are prompted to "Confirm Account" and set a password.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

VA staff – Caregiver Support Coordinators are the only users that have access to the system. Only personnel with a clear business purpose are allowed access to the system and the information contained within. Access control for CoreTech is accomplished through VA Contract Officer Representative confirming completion of background check and TMS trainings. Access control for VA staff is accomplished through portal access requests via active VA email address and confirmation of Caregiver Support Coordinator assignment within the facility.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

VACO Administrators have access to all data in Portal. General users only have access to data within their assigned facilities.

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.

The contractor - CoreTech designed, developed and maintain the NCTP portal. Their staff have access to the system. There is a Business Associate Agreement in place for this contract.

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.

Coretech staff must complete the Privacy and Rules of Behavior training each year.

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

8.4a If Yes, provide:

1. The Security Plan Status: <<ADD ANSWER HERE>>
2. The System Security Plan Status Date: <<ADD ANSWER HERE>>
3. The Authorization Status: <<ADD ANSWER HERE>>
4. The Authorization Date: <<ADD ANSWER HERE>>
5. The Authorization Termination Date: <<ADD ANSWER HERE>>
6. The Risk Review Completion Date: <<ADD ANSWER HERE>>
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH): <<ADD ANSWER HERE>>

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

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

10/20/2024.

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud

models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. **Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)

Microsoft Azure Public Cloud using PaaS models.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Per Azure privacy documentation: "With Azure, you are the owner of the data that you provide for storing and hosting in Azure services. We do not share your data with advertiser-supported services, nor do we mine it for any purposes like marketing research or advertising."

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.

The Caregiver Support Program Office owns the ancillary data.

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 – We have a Business Associate Agreement in place between the VHA and CoreTech Global that establishes roles and responsibilities with respect to HIPAA, HITECH, HIPAA Rules, and PHI.

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).

No RPA’s are used.

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

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

Signature of Responsible Officials

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

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2024.11.20 13:59:43 -05'00'

Privacy Officer, Dennis Lahl

AMINE MESSAOUDI Digitally signed by AMINE MESSAOUDI
Date: 2024.11.20 13:35:39 -06'00'

Information System Security Officer, Amine Messaoudi

KANDACE SMITH Digitally signed by KANDACE SMITH
Date: 2024.11.20 15:08:03 -05'00'

Information System Owner, Kandace Smith

APPENDIX A-6.1

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

For the online application there is a link to View Privacy Act Statement on the page before the Veteran or Caregiver can begin the application. Also on the last page of the online application before submission, the Veterans's Statement of Truth includes the following statement:

I have read and accept the privacy policy (hyperlink must be clicked on). The link for privacy policy takes the applicant to the VA.Gov – Privacy, policies and legal information site (see Appendix A-6.1). The name of the applicant must be entered into the field along with the certification that the information provided is correct and true.

For the paper application, the Privacy Act Information is listed on page 2 of the Please Read Before you Start instruction sheet.

SORN:

197VA10 / 89 FR 6568 - Caregiver Support Program—Caregiver Record Management Application (CARMA)—VA - https://www.govinfo.gov/content/pkg/FR-2024-02-01/pdf/2024-01984.pdf

About VA Form 10-10CG | Veterans Affairs

Privacy, Policies, And Legal Information | Veterans Affairs

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices