



Privacy Impact Assessment for the VA IT System called:

Caregivers Legal and Financial Services
Veterans' Health Administration
Caregiver Support Program
EMASS ID: 2222

Date PIA submitted for review:

4/8/2025

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)	Richard Alomar-Loubriel	Richard.Alomar-Loubriel@va.gov	787-696-4091
Information System Owner	Timothy Jobin	Timothy.Jobin2@va.gov	702-249-2520

Abstract

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

The Caregivers Finance and Legal Services system will serve as a referral portal as well as a location for eligible Caregivers (in support of their Veterans) to access various (public facing) services such as to take finance and legal services training. The system also provides access to, provide webinars. The portal allows users to make appointments for services with attorneys/financial advisors and download templates/worksheets. This portal is a public facing website housed in the VA Enterprise Cloud (VAEC).

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

Caregivers Legal and Financial Services/ VHA Caregiver Support Program serves as a referral portal as well as a location for eligible Caregivers (in support of their Veterans) to access (public facing) to take finance and legal services training, provide webinars, make appointments for services with attorneys/financial advisors, and download templates/worksheets.

- B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

VA owned and non-VA Operated IS by MyRevelations, that operates maintenance of the IT system and housed within VAEC.

2. Information Collection and Sharing

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

Expected number of individuals utilizing the system per year range between roughly 7000 – 9000. The typical client is a caregiver of a Veteran that is enrolled in the Program of Comprehensive Assistance for Family Caregivers. Data elements collected include (for Primary Caregiver and/or Veteran): Full Name, DOB, Address, Email Address, Phone number, time zone, best time to call, preferred language, services requested, Primary VAMC

where receives Care, Home State/US Territory, CARMA number, and any services they are requesting. For VA Staff (CSP staff and Program Managers) First Name, Last Name, Email Address, phone number and VAMC. For contractors: First and Last Name and email address and phone number.

Check if Applicable	Demographic of individuals
<input checked="" type="checkbox"/>	Veterans or Dependents
<input checked="" type="checkbox"/>	VA Employees
<input type="checkbox"/>	Clinical Trainees
<input checked="" type="checkbox"/>	VA Contractors
<input type="checkbox"/>	Members of the Public/Individuals
<input type="checkbox"/>	Volunteers

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

The system will serve as a referral portal as well as a location for eligible Caregivers (in support of their Veterans) to access finance and legal services training, provide webinars, make appointments for services with attorneys/financial advisors, and download templates/worksheets. This portal is a public facing website housed in the VA Enterprise Cloud (VAEC).

E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

None

F. *Are the modules/subsystems only applicable if information is shared?*

None

G. *Is the system operated in more than one site to include primary and secondary 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?*

No, only 1 site.

3. *Legal Authority and System of Record Notices (SORN)*

H. *What is the citation of the legal authority?*

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). Caregiver Support Program— Caregiver Record Management Application (CARMA)—VA’’; SORN: 121VA10P2

[Federal Register :: Privacy Act of 1974; System of Records](#)

I. *What is the SORN?*

Caregiver Support Program— Caregiver Record Management Application (CARMA)—VA’’; SORN: 197VA10

J. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

No

4. *System Changes*

K. *Will the business processes change due to the information collection and sharing?*

Yes

No

if yes, <<ADD ANSWER HERE>>

I. *Will the technology changes impact information collection and sharing?*

Yes

No

if yes, <<ADD ANSWER HERE>>

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 Information 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.

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

- | | | |
|---|---|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Financial Information | <input type="checkbox"/> Number (ICN) |
| <input type="checkbox"/> Full Social Security Number | <input type="checkbox"/> Health Insurance Beneficiary Numbers | <input type="checkbox"/> Military History/Service Connection |
| <input type="checkbox"/> Partial Social Security Number | <input type="checkbox"/> Account Numbers | <input type="checkbox"/> Next of Kin |
| <input checked="" type="checkbox"/> Date of Birth | <input type="checkbox"/> Certificate/License Numbers ¹ | <input type="checkbox"/> Date of Death |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Vehicle License Plate Number | <input type="checkbox"/> Business Email Address |
| <input checked="" type="checkbox"/> Personal Mailing Address | <input type="checkbox"/> Internet Protocol (IP) Address Numbers | <input type="checkbox"/> Electronic Data Interchange Personal Identifier (EDIPI) |
| <input checked="" type="checkbox"/> Personal Phone Number(s) | <input type="checkbox"/> Medications | <input checked="" type="checkbox"/> Other Data Elements (List Below) |
| <input type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Medical Records | |
| <input checked="" type="checkbox"/> Personal Email Address | <input type="checkbox"/> Race/Ethnicity | |
| <input type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a Different Individual) | <input type="checkbox"/> Tax Identification Number | |
| | <input type="checkbox"/> Medical Record Number | |
| | <input type="checkbox"/> Sex | |
| | <input type="checkbox"/> Integrated Control | |

Other PII/PHI data elements: (Veterans or Dependents) CARMA number, Primary VAMC, Home State/US Territory, Time Zone, What services the person wants to receive (VA Employees) First Name,

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

Last Name, Email Address, phone number and VAMC; and (Contractors) First and Last Name and email address and phone number

1.2 List 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?

The information will be collected from one of four sources: Caregivers, Veterans, Care Concierge and Caregiver Support Program Team staff.

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.

Information will be required from VA Caregiver Support Program Team staff in order to validate eligibility for the services and formally make a referral for such services.

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

None- (only reports directly from this site would include non PII specific site metrics/web analytics— i.e., how busy site is and how many people benefiting from site)

1.3 Methods of information collection

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

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

From an individual (i.e., Caregiver, Veteran, Caregiver Concierge or Caregiver Support Program Team/staff/Program Managers, etc.)

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?

Information is not collected on a form.

1.4 Information checks for accuracy, and how often will it be checked.

Version date: October 1, 2024

Page 6 of 31

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.

Refer to information captured directly from the Veteran, Caregiver, Caregiver Concierge or Caregiver Support Program Team and assumed to be accurate. The Caregiver Support team will validate the information and provide the CARMA number for verification of eligibility. Approval is valid for website access for a period of 1 year.

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 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

The 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.

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: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

*Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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: Caregiver Finance and Legal Services collects PII. Due to the sensitive nature of this data, there is a risk that if the data were accessed by an unauthorized individual or otherwise breached, it could be exposed.

Mitigation: The information that is collected is only used to validate that the subject is approved to use the Caregivers Financial and Legal services web site resources and is not used for any follow-on purpose.

- The information collected is only the minimum needed in order to validate the subject eligibility to use the Caregivers Financial and Legal services web site resources.
- Any inaccurate information entered the system will not cause failure in approving eligibility for a subject as there is more than a single piece of PII that can be utilized to prove subject eligibility.
- Once eligibility to utilize the Caregivers Financial and Legal services site is established, accuracy of the data stored in the system is no longer critical and does not need to be maintained as no contact will be made to the subject using data from this system.

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	File Identification purposes: Information primarily needed	Not used

Date of Birth Personal Mailing Address Personal Phone Number Personal Email Address Name Date of Birth Personal Mailing Address Personal Phone Number Personal Email Address Other PII Elements : (Veterans or Dependents) CARMA number, Primary VAMC, Home State/US Territory, Time Zone, What services the person wants to receive (VA Employees) First Name, Last Name, Email Address, phone number and VAMC; and (Contractors) First and Last Name and email address and phone number	to verify eligibility for services.	
--	--	--

2.2 Describe the types of tools 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 provided primarily for registration and authentication of eligibility and not for analysis.

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.

No derivative information being created.

2.3 How the information in the system is 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 at rest is Encrypted by Amazon RDS database service and Data in transit is encrypted by TLS.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Not collecting SSN.

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

Role Based Access, Verification of eligibility prior to access, and mandatory onboarding/TMS training where applicable (Contractors directly working with VA data follow contract language related to onboarding/background checks as well as meeting the minimum HIPPA/Rules of Behavior training requirements prior to access). Technical controls include hosting in the VA Enterprise Cloud (VAEC) and inheriting Physical and Technical safeguards from AWS and VAEC. In addition to following all applicable VA procedures and regulations which are FISMA compliant.

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?

Access is determined by the CSP Team at the caregiver's VAMC based on eligibility requirements for Primary Family Caregiver. Only personnel required to complete the contract are eligible for onboarding. Per contract, those that directly interface with VA data are required to meet basic onboarding requirements (such as for those that receive information directly from the VA must receive the corresponding background checks and complete the mandatory TMS

HIPAA/Rules of Behavior training, etc.). VAMC CSP Team members will be required to maintain standard VA TMS requirements and will receive restricted role-based access. Vendors will also have role-based access limitations based on the corresponding job/role.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Project plan (MyRevelations) documents who is a part of the contract and the HR contract maintains a list of who has background checks/PIVs, etc. (as does the COR) to document which vendors have been onboarded to the contract. There is a Primer document that describes the eligible resources and mechanism for access that will be provided in training venues with the VAMC CSC Teams.

2.4c Does access require manager approval?

Yes

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

Yes, access to each page and record is tracked in the WordPress logs and the user accessing is called out by username.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

Administrative managers, system users, Concierges, and system administrators. (As an example, when a caregiver selects a medical center as the primary center for care, the system will only alert CSP Team members to log in and review referral requests for unvalidated Caregivers at their location.... once verified, then that CSC Team will no longer have access to that data.)

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*

Data elements collected include (for Primary Caregiver and/or Veteran): Name, Date of Birth, Personal Mailing Address, Personal Phone Number, Personal Email Address. Other PII Elements: (Veterans or Dependents) CARMA number, Primary VAMC, Home State/US Territory, Time Zone, What services the person wants to receive (VA Employees) First Name,

Version date: October 1, 2024

Page 11 of 31

Last Name, Email Address, phone number and VAMC; and (Contractors) First and Last Name and email address and phone number .

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 <https://www.archives.gov/records-mgmt/grs>? This question is related to privacy control DM-2, Data Retention and Disposal.

Caregiver Finance and Legal Services complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the VAEC Amazon database will be retained if the information is needed in accordance with a NARA-approved retention period. MyRevelations manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFDP records are retained according to Record Control Schedule 10-1 Section 4. Record Control Schedule 10-1 can be found here, specifically 2201.2 for Intermediary Records: <https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf>.

Account information for the CFS LFS website will be retained for 1 year and 2 weeks.

3.3 The retention schedule 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. Please work with the system VA Records Officer to answer these questions. This question is related to privacy control DM-2, Data Retention and Disposal.

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

Yes. 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 is found at this link: <https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>

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

Caregiver web site user information is retained for as long as that user is approved and is actively interacting with the web site. Furthermore, sensitive user information such as DOB are only retained as Transitory records for as long as that data is require to establish a CARMA number as

is refereed by SORN 197VA10 states General Records Schedule approved 5.2 item 20 by NARA <https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf>.

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.

Per Contract: Upon completion or termination of the applicable contract(s) or agreement(s), return or destroy all PHI and other VA data created or received by Business Associate during the performance of the contract(s) or agreement(s). No such information will be retained by Business Associate unless retention is required by law or specifically permitted by Covered Entity. If return or destruction is not feasible, Business Associate shall continue to protect the PHI in accordance with the HIPAA Rules or this Agreement and use or disclose the information under this Agreement only for the purpose of making the return or destruction feasible, as required by law, or as specifically permitted by Covered Entity. Business Associate shall provide written assurance that either all PHI has been returned or destroyed, or any information retained will be safeguarded and used and disclosed only as permitted under this paragraph.

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.

This system does not use this PII for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document in 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

*Principle of Data Quality and Integrity: The PIA should describe 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: Unintended access to PII or unintended data breach

Mitigation: Role based access is primary process to reduce exposure to PII. In addition, referrals only remain active for 1 year and post the 1 year, the caregiver information is only accessible by the help desk team. Once accounts are approved, the CSP Team at local VAMCs are no longer able to access the account records. Information is not retained longer than needed by the organization which is 1 year and 2 weeks and does not include the sensitive PII data type, only name, address, phone number, CARMA number, email address, and Primary VAMC. By reducing the type of PII retained using transitional records as detailed in the RCS-10-1, the organization is reducing the risk of what type of PII is susceptible to an unintended breach or access.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a Caregiver Finance and Legal Services consists of 1 key components (Public facing web service portal). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Caregiver Finance and Legal Services 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 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software,	Does this system collect PII? (Yes/No)	Does this system store	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
--	---	-------------------------------	-------------------------------------	--	-------------------

Application Program Interface (API etc.) that contains PII/PHI		PII? (Yes/No)			
Caregiver Finance and Legal Services	Yes	Yes	<p>Caregiver and/or Veteran) DOB, Name, Address, CARMA number, personal phone, personal email, Primary VAMC, Home state/US Territory, Time Zone, and what services the person wants to receive.</p> <p>For VA Staff (CSP and PM) First Name, Last Name, VA email address, phone number and VAMC. for contractors: First and Last Name and email address and phone number</p>	Authenticate authorized users for the caregiver Finance and Legal Services system	Accounts expire annually (every 365 days), and accounts are hand approved by the CSP team at the VAMC and limit exposure to PII through Role Based Access. The database for the Caregiver Legal and Financial Services application is stored on Amazon AWS (Amazon Web Services) Relational Database Service (RDS), inside the VA Enterprise

					<p>Cloud (VAEC). As such it inherits all security controls managed by AWS, RDS, and VAEC ATO's. All data in the database is stored in volumes that are encrypted at rest, and all queries between the application and the database are encrypted in transit using standard TLS.</p> <p>encryption. Access to the database is restricted by IP address to only the single application web server that requires access and is further restricted by username and</p>
--	--	--	--	--	--

					password. All data is backed up daily using the regular RDS backup process. Privileged access to the VAEC environment is restricted to dedicated admin virtual machines and bastion hosts, and user accounts that are not connected to an e-mail address to protect against malware and ransomware attacks.
--	--	--	--	--	--

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

<i>IT system and/or Program office. Information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List PII/PHI data elements shared/received/transmitted.</i>	<i>Describe the method of transmittal</i>
None	None	None	None

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized personnel. Data is used to ultimately manually create a new entry in other system post initial access call/contact once data is validated.

Mitigation: The information is not shared in a physical/electronic manner—rather it is manually entered into the external system and validated by the person completing the intake.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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.

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

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

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

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

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

Data Shared with External Organizations

<i>List IT System or External Program Office information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)</i>	<i>List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
None	None	None	None	None

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: There is no external sharing.

Mitigation: There is 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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

The following privacy notice is posted on the login page of the Caregiver Finance and Legal Services website: 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.

6.1b If notice was not provided, explain why.

Notice was provided.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Caregivers/Veterans logging into the system will see the privacy act statement and understand their information will be protected accordingly.

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.

Yes. Individuals are not mandated to fill in the information on the website. If they are not willing to enter directly onto the website, they can be referred to the local CSC Team who can input the referral or refer them directly to a concierge if they only want live services versus web based.

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.

No—but information only used to validate identify for verification of eligibility.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: Unintended use of information, Incorrect information will conflict with internal VA system which can cause delay of receipt of services until validated by VA Staff There is a risk that an individual may not receive the VHA Notice of Privacy Practice (NOPP) that their information is being collected, maintained, processed, or disseminated by the Veterans Health Administration prior to providing the information to the VHA.

Mitigation: Technical controls and business processes minimize the risk of using the data for purposes other than the intended purpose of confirming eligibility. This risk is mitigated by the common practice of providing the VHA Notice of Privacy Practice (NOPP) when Veterans apply for benefits. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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 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 [VA Public Access Link-Home \(efoia-host.com\)](http://vafoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Requestors may submit a FOIA request. Submitting a written FOIA request signed by the requestor(s) and reasonably describing the records sought to the VHA Central Office FOIA Service at 810 Vermont Avenue, NW (10A7) Washington, DC 20420, by fax at 202-273-9381, or via email at vhafoia2@va.gov. The VHA FOIA Office will obtain the requested records from the VHA Compliance and Business Integrity Office and respond to the request as appropriate. Per the Privacy Act, only the subject of the record (First Party Access) or appropriate designee (Third Party Access) can request information. In addition, Information collected may be shared with VHA employees, contractors, and other service providers as necessary to respond to a request, provide a service, administer clinical treatment, solicit payment or as otherwise authorized by law. Information will not be shared with, or accessible by, any other entity without prior approval from CBI and review of data security and safety plans.

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)?

The system is not exempt from the access provisions of 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?

The system is a Privacy Act system.

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

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

An individual who seeks to correct inaccurate or erroneous information or wishes to contest records maintained under his or her name in this system may write, call the MyRevelations Liaison Customer Service Team.

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

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

An individual who seeks access to or wishes to contest records maintained under his or her name in this system may write, call the MyRevelations Liaison Customer Service Team.

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

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

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

None.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There could be errors that the person does not alert the help desk, so they remain. There is a risk that individuals whose records contain incorrect information may not receive access to assistance in a timely manner.

Mitigation: Link at the bottom of every page where the member can contact the help desk.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

Administrative users are granted cloud access via Electronic Permission Access System;
Caregiver application users are granted access by manager and/or regional supervisors;

caregivers are granted access through referral. Per contract, in relation to contractor access, “All Contractors and Contractor personnel working directly with the VA in support of this contract (as prime contractors/prime contractor staff) shall be subject to the same Federal security and privacy laws, regulations, standards and VA policies as VA personnel, including the Privacy Act, 5 U.S.C. § 552a, regarding information and information system security. Contractors must follow all security and privacy requirements, per 6500 Attachment C - VA Information and Information System Security/Privacy requirements. During active performance Contractors and Contractor personnel are responsible for maintaining compliance with VA policies.”

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?

Users from other agencies are not granted access.

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.

Application administrators, Help Desk, Caregivers, Caregiver Support Program Team members and supervisors. Access to the cloud infrastructure is limited to administrative roles.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Yes

8.2a. Will VA contractors have access to the system and the PII?

Yes

8.2b. What involvement will contractors have with the design and maintenance of the system?

A Business Associate Agreement is on file with MyRevelations and Three-Wire Systems where contractor will performing design improvements, application and system upgrades along with patching of the information system.

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.

The contractors are required to complete TMS 10176 and TMS 10203. In addition, those requiring elevated privileges complete the TMS course titled Elevated Privileges for System Access. For those working directly with the VA/Veterans Health Administration, the staff will be required to complete the full Background Check process (to include corresponding document submission, fingerprint check, and favorable adjudication) as well as maintain the annual training requirements through the Talent Management System (to complete minimum corresponding VA training requirements to include (TMS 10176) TMS VA Privacy and Information Security Awareness and Rules of Behavior course along with the (TMS 10203)TMS VA Privacy and HIPAA Training Course) prior to gaining access to VA information. VA staff (GS employees) will follow the standard annual TMS training requirements per VHA policy related to HIPAA/Privacy training requirements.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

- 1. The Security Plan Status: Completed*
- 2. The System Security Plan Status Date: 4/3/25*
- 3. The Authorization Status: Authority to Operate*
- 4. The Authorization Date: 5/10/2024*
- 5. The Authorization Termination Date: 5/10/2025*
- 6. The Risk Review Completion Date: 5/9/2024*
- 7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Moderate*

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 not completed or In Process, provide your **Initial Operating Capability (IOC) date.***

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

Version date: October 1, 2024

Page **26** of **31**

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. **(Refer to question 1.8 of the PTA)**

VAEC Amazon Web Services (VA cloud web services)

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Not required as the system is utilizing VAEC.

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 system does not collect 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.

Not required as the system is utilizing VAEC.

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).

The system does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

Privacy Officer, Dennis Lahl

Information System Security Officer, Richard Alomar-Loubriel

Information System Owner, Timothy Jobin

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).

The following will be posted on the login page: 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.caregiverfinanciallegal.va.gov/register/>

<https://www.caregiverfinanciallegal.va.gov/login/>

HELPFUL LINKS:

[Records Control Schedule 10-1 \(va.gov\)](#)

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 Directive 1605.04

[IB 10-163p \(va.gov\)](#)