Privacy Impact Assessment for the VA IT System called:

Salesforce – Medical Foster Homes

Veterans Health Administration

Patient Care Services – Geriatrics and Extended Care

eMASS ID # 2500

Date PIA submitted for review:

05/24/2024

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)	James Boring	James.Boring@va.gov	215-842- 2000, Ext: 46
Information System Owner	Michael Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

The abstract provides the simplest explanation for "what does the system do?".

The Salesforce – Medical Foster Homes (SF-MFH) system will give VHA facilities the ability to manage Medical Foster Home Caregiver and Veteran data required by the Cleland Dole Act, Section 165. Using Single Sign-on (SSOi), SF – MFH will track Caregiver background checks and applications, as well as denials and approvals. The system will also track payment data, to include the rates charged. Annual inspections and education and training completed by caregivers will be tracked. Veteran demographics and benefit/eligibility information will be collected from VA Profile to facilitate assignment to caregivers.

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?

Salesforce Government Cloud Plus (SFGCP) is a cloud AWS environment owned by VA. This particular minor app Salesforce – Medical Foster Homes (SF-MFH) is under the control of VHA's Patient Care Services – Geriatrics and Extended Care program office.

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 Salesforce – Medical Foster Homes (SF-MFH) system will give VHA facilities the ability to manage Medical Foster Home Caregiver and Veteran data required by the Cleland Dole Act, Section 165. The system will act as a repository for all of the participating facilities Medical Foster Home's data collected to be presented to VHA leadership through dashboard and reporting.

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

Salesforce Government Cloud Plus (SFGCP) is a cloud platform, data in the platform is controlled by VA but non-VA Owned and Operated. VA has sole ownership of the information and data located in Salesforce's Data Center. Authorized VA employees and VA contractors have access to the data available in SF-MFH

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?

The expected number of veterans who will have information stored in the MFH system will initially be 750 and increase over time. The typical affected individual is a veteran who meets the criteria for consideration to stay in a Medical Foster Home.

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

SF-MFH provides a more comprehensive and integrated approach to caregiver record management by streamlining existing processes and providing improved reporting capability. The system will track:

1. Caregiver applications, to include whether a background check has been completed, as well as denials and approvals.
2. Payment data and rates charged.
3. Annual inspections and education and training completed by caregivers.

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

Information Sharing for SF-MFH is as follows:

Master Person Index (MPI) for search and identification verification of the Veteran and of the Caregiver.

VA Profile to receive and share address and phone number updates, receive benefit status and service-connected information, and access Enrollment & Eligibility (E&E) to retrieve Veteran information to assist in determining eligibility in the program.

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?

SF-MFH is a single cloud-based system. PII maintenance across multiple sites is done through 1. data at rest and at transit is encrypted. SFGCP utilizes FIPS 140-2 shield encryption. 2. multifactor authentication using PIV ensuring only authorized users have access to PII.

SF-MFH is a minor application which leverages security controls from SFGCP-E package. The security controls protecting the PII data within VA Salesforce are documented in the approved SFGCP-E Authority to Operate (ATO). VA Salesforce is leveraging the security controls as part of the common services offered by Amazon Web Services (AWS). The specific security controls leveraged by VA Salesforce, in addition to a detailed description of the SFGCP-E/Salesforce security boundaries, are documented in the VA SFGCP-E System Security Plan (SSP).

Salesforce Government Cloud Plus (SFGCP-E) is maintaining underlying physical infrastructure. Additional ISA/MOUs are required between the VA and VA designated contractors/vendors that access the data that is stored or processed within Salesforce Development Platform VA. The vendor-specific agreements will describe the data ownership and storage requirements. The parties agree that transmission, storage and management of VA sensitive information residing in the SFGCP-E is the sole responsibility of VA employees or designated contractors/vendors assigned to manage the system. At no time will Salesforce Government Cloud have any access to VA data residing within Salesforce Government Cloud Plus. Thus, all agreements on data and system responsibilities shall not be covered in this base agreement (MOU). However, Salesforce Government Cloud shall provide the tools to allow VA to properly secure all systems and data hosted in SFGCP-E.

3. Legal Authority and SORN

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

This list is the full list of related laws, regulations and policies and legal authorities:

- Title 38, United States Code, Sections 501(a), 1705, 1710, 1720, 1722, and 53

- Information from the SORN: The Department of Veterans Affairs provides additional notice of this system by publishing the following System of Record Notice (SORN):
  - The VA System of Record Notice (VA SORN) Community Residential Care and Medical Foster Home Programs VA, SORN 142VA10 (July 28, 2023) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/conten/pkg/FR-2023-07028/2023-16020.pdf
  - The VA System of Record Notice (VA SORN) Caregiver Support Program – Caregiver Record Management Application (CARMA), SORN 197VA10 (April 9, 2021) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2021-04-09/pdf/2021-07310.pdf
  - National Patient Databases-VA SORN 121VA10 / 88 FR 22112 is available in the Federal Register and online. An online copy of the SORN can be found at https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf
- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law
- No. 104---231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- E-Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites
- OMB Memo M---99---18, Privacy Policies on Federal Web Sites
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- VA Directive and Handbook 6502, Privacy Program
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws

The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 939.

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?*

The system is not in the process of being modified. The system uses cloud technology and is covered in these SORNs.

The VA System of Record Notice (VA SORN) Community Residential Care and Medical Foster Home Programs VA, SORN 142VA10 (July 28, 2023) is available in the Federal

Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/conten/pkg/FR-2023-07028/2023-16020.pdf

The VA System of Record Notice (VA SORN) Caregiver Support Program – Caregiver Record Management Application (CARMA), SORN 197VA10 (April 9, 2021) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2021-04-09/pdf/2021-07310.pdf

National Patient Databases-VA SORN 121VA10 / 88 FR 22112 is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

4. System Changes

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

No, the completion of this PIA will not result in changes to business processes.

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

No, the completion of this PIA will not result in technology changes.

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 (list below)

Other PII/PHI data elements:

- Service-Connected percentage Total
- Vendor ID Number (Caregiver Payee ID)
- Benefit Status
- Enrollment and Eligibility
- Medical Foster Home Stay Start and End Dates
- Financial Payment Data
- Caregiver Relationship to Veteran
- Training and/or Certification Data
- Home Inspection Data

PII Mapping of Components (Servers/Database)

Salesforce – Medical Foster Homes consists of 3 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Salesforce – Medical Foster Homes 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
MPI – Master Person Index	Yes	Yes	Name, Veteran Unique ID, DOB, Address, Personal Phone, Personal Email, Suffix	Search and identification verification of Veteran and Caregiver	Sends and receives data through REST/JSON via HTTPS to the Digital Transformation Center Integration Platform (DIP)
VA Profile	Yes	Yes	Name, Veteran Unique ID, DOB, Address, Personal Phone, Personal Email, Suffix, Benefit Status, Enrollment & Eligibility, Gender Identity	Search and identification verification of Veteran and Caregiver	Sends and receives data through REST/JSON via HTTPS to the Digital Transformation Center Integration Platform (DIP)
SSOi	Yes	Yes	Name, Veteran Unique ID, Personal Email	Search and identification verification of Veteran and Caregiver	Electronic Transfer using Secure Socket Layer (SSL) Encryption

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?

The information listed above is collected and shared from both Veterans and Caregivers through the application process for the program and through enrollment for the program. In addition, SF-MFH utilizes the VA enterprise systems of record for validating and verifying information such as the use of MPI for identity management and VA Profile for address validation, benefit status, enrollment and eligibility and gender identity.

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.

SF-MFH utilizes the VA enterprise systems of record for validating and verifying information such as the use of MPI for identity management and VA Profile for address validation and benefit status.

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

SF-Medical Foster Homes is a source of information which will allow creation of dashboard and report for VHA leadership oversight.

1.3 How is the information collected?
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?

The information and data will be collected through validation of the data provided by IAM and their access to the Master Person Index (MPI) and the VA Profile API.

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?

The information will be collected electronically and not on a form.

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.

SF-MFH uses the VA Profile address validation service to ensure addresses entered into the system are accurate and deliverable. Addresses are validated when data is initially stored and ad hoc whenever VA personnel have validity concerns. Information for the Master Person Index (MPI) is managed by the respective VA enterprise services and changes to data is provided to SF-MFH near real-time. SF-MFH is a read-only consumer of this data.

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?

SF-MFH does not use a commercial aggregator to check for accuracy.

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

The following is a full list of related laws, regulations and policies and the legal authorities:

- Title 38, United States Code, Sections 501(a), 1705, 1710, 1720, 1722, and 53
- Information from the SORN: The Department of Veterans Affairs provides additional notice of this system by publishing the following System of Record Notice (SORN):
    - The VA System of Record Notice (VA SORN) Community Residential Care and Medical Foster Home Programs VA, SORN 142VA10 (July 28, 2023) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/conten/pkg/FR-2023-07028/2023-16020.pdf
    - The VA System of Record Notice (VA SORN) Caregiver Support Program – Caregiver Record Management Application (CARMA), SORN 197VA10 (April 9, 2021) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2021-04-09/pdf/2021-07310.pdf
- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law
- No. 104---231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- E-Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites

- OMB Memo M---99---18, Privacy Policies on Federal Web Sites
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- VA Directive and Handbook 6502, Privacy Program
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State Privacy Laws

The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 939

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. (*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.

Follow the format below when entering your risk assessment:

Privacy Risk: Sensitive Personal Information (SPI) including personal contact information, SSN and medical information may be released to unauthorized individuals. Unsecured Sensitive Personal Information (SPI) including personal contact information, SSN and medical information may be exposed. Data breach at the facilities level. Data breach at the network level.

Mitigation: Depending on level of authority granted to the respective user by their home department via the VA, each user will have sensitivity level of access to veteran data based on role-based permissions. The roles will be reviewed on a regular basis to ensure that appropriate information is shared with appropriate users. All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually.

To mitigate risk, Salesforce Development Platform protects data by ensuring that only authorized users can access it. Data security rules are assigned that determine which data users can access. All data is encrypted at rest and in transfer. Access is governed by strict password security policies. All passwords are stored in Secure Hash Algorithm (SHA) 256 one-way hash format.

To ensure the utmost privacy and security at the facility level, authorized personnel must pass through multiple levels of biometric and/or badge scanning to reach the Salesforce system rooms/cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of a suspected intrusion. Data is backed up. Backups do not physically leave the data center.

Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only https traffic on port 443, along with Internet Control Message Protocol (ICMP) traffic. Switches ensure that the network complies with the Request for Comment (RFC) 1918 standard, and address translation technologies further enhance network security. Intruder Detection & Protection System (IDPS) sensors protect all network segments of data for minor apps inherit the major platform's controls. This is included as a mitigation for data breach at a network level. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system 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	Identify the Veteran who is housed in a MFH or applying for one Identification of Caregiver providing support to the Veteran Identification of VA employee accessing the SF-MFH system	Not used
Veteran Unique ID (could be SSN)	Identification	Not used
Date of Birth	Identification	Not used
Mailing Address	Contact	Not used
Personal Phone	Contact	Not used

Email address	Contact	Not used
Gender Identity	For care-associated use	Not used
Service-Connected Percentage Total	Eligibility	Not used
Benefit Status	Eligibility	Not used
Enrollment and Eligibility	Eligibility	Not used
Medical Foster Home Start and End Dates	Payment	Not used
VA Employee Name	Identification and contact	Not used
VA Employe Email	Identification and contact	Not used
Caregiver Name	Identification and contact	Not used
Caregiver Address	Contact	Not used
Caregiver Phone	Contact	Not used
Caregiver Email	Contact	Not used
Caregiver SSN	Identification	Not used
Vendor ID Number (Caregiver Payee ID)	Payment	Not used
Caregiver Relationship to Veteran	Identification	Not used
Training and/or Certification data	Qualifications	Not used
Home Inspection data	Qualifications	Not used
Financial Payment Data	Payment	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?

Salesforce is used to run reports. SF-MFH users are presented with a series of standard reports that provide data in different views depending on user role for VHA leadership oversight. No analysis or manipulation of data is conducted.

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 create or make available new or previously unutilized information about an 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 is encrypted. Data in standard field objects within the Salesforce Government Cloud Plus are encrypted at rest and in-transit. SF-MFH specific objects are made available only to certain users through role-based permissions.

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

The SSN field standard contact object is encrypted at rest and in-transit through FIPS 140-2 encryption. The SSN field used on the SF-MFH Contact Relationship object is available only to certain users through role-based permissions.

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

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA and Salesforce have implemented required security and privacy controls for Federal Information Systems and Organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for Information Technology [the VA Designated Accrediting Authority (DAA)].

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

<u>Principle of Use Limitation:</u> 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?

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately.

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

VA and Salesforce have implemented required security and privacy controls for Federal Information Security Modernization Act (FISMA) according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.
New users submit a request for access through the Digital Transformation Center (DTC). DTC then assigns the request to the individuals who have admin access to the module and the access is then granted or denied based on the information the user provided by the admin. DTC is then notified of the approval/disapproval while DTC takes action on the request based on the admin's response. Requests, approvals, and denials of access are recorded within Salesforce-VA Help Desk application.

2.4c Does access require manager approval?

Yes, managerial approval is required of the Acting Assistant Secretary for information Technology [the VA Designated Accrediting Authority (DAA)].

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

Yes, VA Identify and Access Management (IAM) systems verify credentials and collect audit logs based on access requested and may contain PII that might have been captured to authenticate to the resource.

Salesforce has implemented required security and privacy controls for Federal Information Systems and Organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for information Technology [the VA Designated Accrediting Authority (DAA)].

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

Accessibility to data is granted based on the permission sets and role-based hierarchy applied based on FedRAMP Salesforce Gov Cloud Plus platform. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card and/or Access VA. Single Sign On external (SSOe) is used to provide credential access to VA modules/communities residing in the Salesforce application, the determinant of access is organizational affiliation rather than personal identity. For some module(s) the required organizational e-mail confirmation and multi-factor authentication (MFA) will be enforced (IAL1), but no identity proofing (IAL2) and vice versa. The managers will reject any applications from individuals who do not work with them, do not require access or are not using the correct e-mail address. IAM systems verify credential and collect audit logs based on access requested and may contain PII that might have been captured into order to authenticate to the resource.

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*

- Veteran Name
- Veteran Unique ID Number (May be Social Security Number)
- Veteran Date of Birth
- Veteran Address
- Veteran Personal Phone
- Veteran Personal Email
- Veteran Gender
- Veteran Service-Connected Percentage Total
- Vendor ID Number (Caregiver Payee ID)
- Veteran Benefit Status
- Veteran Enrollment and Eligibility
- Veteran Medical Foster Home Stay Start and End Dates
- Veteran Financial Payment data
- VA Employee Name
- VA Employee Email
- Caregiver Name
- Caregiver Address
- Caregiver Phone
- Caregiver Email
- Caregiver Social Security Number
- Vendor ID Number (Caregiver Payee ID NPI)
- Caregiver Relationship to Veteran
- Training and or Certification data
- Home Inspection data
- Financial Payment data

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *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.*

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 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.

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.

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

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

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

VA 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). SFGCP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records): https://www.va.gov/vhapublications/RCS10/rcs10-1.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.

Active Data stays on disk until the VA deletes or changes it. Data on backups is retained for 90 days until the backups are overwritten. Log data is retained by Salesforce for a year. VA exports data and retain it to meet VA/NARA retention requirements and dispose of the exported data at the end of the retention period. When hard drives and backup tapes are at their end of life, the media is sanitized based on Salesforce's Media Disposal Policy. Hard drives are overwritten using a multiple---pass write of complementary and random values. If it wipes successfully, we will return the disk or array to the vendor. If it fails during the wiping process we retain and destroy (i.e., degauss, shred, or incinerate). Backup tapes are degaussed prior to disposal. Specifics on the sanitization process are below. Salesforce has an established process to sanitize production backup disks and hard drives prior to disposal, release out of salesforce's control, or release to the vendor for reuse. Production backup disks and hard drives are sanitized or destroyed in accordance with salesforce's Media Handling Process. All data is handled and located in VA own Salesforce's servers in the Salesforce Government Cloud server classification. Said information is handled with proper authority and scrutiny. Hard drives are sanitized within the data center facility using a software utility to perform a seven---pass overwrite of complementary and random values. If the drives wipe successfully, the hardware will be returned to the lessor. If the drive fails during the wiping process the drives are retained within a locked container within the salesforce data center facilities until onsite media destruction takes place. Leasing equipment provides Salesforce with the opportunity to use the latest equipment available from vendors. Periodically, a third-party destruction vendor is brought on---site to perform physical destruction of any hard drives that failed overwrite. A certificate of destruction is issued once the media is physically destroyed. Electronic data and files of any type, including PII, Sensitive Personal Information (SPI), and more are destroyed in accordance with the Department of Veterans' Affairs VA Directive 6500 (February 24, 2021), https://www.oprm.va.gov/docs/Handbook_6500_24_Feb_2021.pdf). When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. The OIT Chief/CIO will be responsible for identifying and training OIT staff on VA media sanitization policy and procedures. The ISO will coordinate and audit this process and document the audit on an annual basis to ensure compliance with national media sanitization policy.

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.

PII is not used for research, testing or training. A "scrubbed" subset of data or "dummy" data is utilized.

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 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?
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 SFGCP is that longer retention times increase the risk that information can be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, the SFGCP adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the team will carefully dispose of the data by the determined method as described in question 3.4. All electronic storage media used to store, process, or access VA records will be disposed of in adherence with the latest version of VA Handbook 6500.1, Electronic Media Sanitization.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
MPI – Master Person Index	Identification of Veteran and Caregiver	• Name • Veteran Unique ID Number (May be Social Security Number) • Date of Birth • Address	API-based, one-way TLS and a JWT token flow

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***
		• Personal Phone • Personal Email • Suffix	
VA Profile	Identification and Eligibility of Veteran	• Veteran Unique ID Number (May be Social Security Number) • DOB • Personal Email • Benefit Status • Enrollment and Eligibility • Address • City • State • Zip code • Phone Number • Marital Status • Gender Identity	API-based, one-way TLS and a JWT token flow
SSOi		• Name • Veteran Unique ID Number (may be Social Security Number) • Personal Email	Electronic Transfer using Secure Socket Layer (SSL) Encryption

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: There is a risk that information may be shared with unauthorized VA personnel.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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:

<u>Privacy Risk:</u> No external sharing.

<u>Mitigation:</u> 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, individuals are provided Privacy Notices for this system in multiple ways.

1) The Department of Veterans Affairs provides additional notice system by publishing the following System of Record Notices (SORN):

- The VA System of Record Notice (VA SORN) Community Residential Care and Medical Foster Home Programs VA, SORN 142VA10 (July 28, 2023) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/conten/pkg/FR-2023-07028/2023-16020.pdf

- The VA System of Record Notice (VA SORN) Caregiver Support Program – Caregiver Record Management Application (CARMA), SORN 197VA10 (April 9, 2021) is available in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2021-04-09/pdf/2021-07310.pdf.

2) The SF-MFH registration site contains a link to the Privacy Policies and Legal Information Page.

3) This Privacy Impact Assessment (PIA) also serves as notice of the system. As required by the eGovernment Act of 2002, Pub.L.107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." It can be found at this website: https://www.oprm.va.gov/privacy/pia.aspx

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Notice was provided and a copy is linked above in 6.1a.

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.

The Notice of Privacy Practice (NOPP) referenced in Appendix A, is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that the individual read and understood the NOPP is scanned into each applicant's electronic file. When updates are made to the NOPP, copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis. The Veteran provides user level data, which may contain PII, for provisioning and providing the salesforce service, and the Customer continues to have access to such information. VA does not otherwise share this information with Salesforce except if required by law to do so. VA has sole ownership of the information and data located in Salesforce's Data Center. VA is the only entity that has access to that said data. Salesforce's Master Subscription Agreement addresses the protection of Customer Data. A sample Master Subscription Agreement can be viewed at http://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf. In addition to the Master Subscription Agreement, Salesforce has documented a System Security Plan that identifies the security controls that Salesforce has documented to protect the environment in which Customer

Data is stored. Additionally, their privacy and security statements can be viewed at http://www.salesforce.com/company/privacy. Salesforce has a Global Privacy Team who oversees privacy for salesforce. Protecting the security and privacy of user data is a shared responsibility between Salesforce and VA that provision user accounts, as stated in the Salesforce Security Guide (https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/salesforce_security_guide.htm).

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.

VHA Handbook 1605.01 'Privacy and Release Information', Section 5 a. (8) 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 Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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.

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: 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 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?

<u>Principle of Use Limitation:</u> 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 will not know that applications built on the SFGCP collect, maintain, and/or disseminate Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

Mitigation: The SFGCP Integrated Project Team (IPT) mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the methods discussed in question 6.1. The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and the SORN.

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://department.va.gov/foia to obtain information about FOIA points of contact and information about agency FOIA processes.***

> VHA Handbook 1605.01 'Privacy and Release Information', Section 5 a. (2) states the rights of the Veterans to request access to review their records. VA Form 10-5345, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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 SF-MFH system is not exempt.

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?

SF-MFH 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.

Veterans submit user level data for provisioning and providing the Salesforce service. The Veteran is responsible for maintaining the accuracy of the data so that the Salesforce services can be provided. This information is collected for the purposes of contracting with or providing services to Veterans and is captured in the normal course of conducting business. The Veteran should correct or update the data as necessary. Under the jurisdiction of VHA, VHA Handbook 1605.01 'Privacy and Release Information', Section 5 a. (3) states the rights of the Veterans to amend their records via submitting VA Form 10-5345, Request For And Authorization to Release Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reasons for this belief. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy office, or designee, to be date stamped; and to be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

Notification for correcting the information must be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations that had previously received the record about the amendment. If 38 U.S.C. 7332- protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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.

The system is designed so that the self-service features are optional. Alternatively, Operations Managers and Providers can update information on the Veteran’s behalf. If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes that previously provided.

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 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 whose records contain incorrect information may not receive notification of any changes. Furthermore, incorrect information in a Veteran's record may result in improper identification.

Mitigation: SF-MFH mitigates the risk of incorrect information in an individual's records by authenticating information and validating data accuracy using the resources discussed in question 1.5. Privileged users such as Providers and Operation Managers will have access to online records other than their own, consistent with their authority and organizational affiliations using PIV.

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?

SNOW ServiceNow will be used to process access to the SF-MFH system. Within SFGCP, user roles identify the information and applications a user can access. To receive access to the SF-MFH, another user of the SF-MFH with appropriate permissions must sponsor them. The sponsor will describe which applications the user needs to access, the user's role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level access of the information and data. This information is documented in the user provisioning process with the Digital Transformation Center (DTC).

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?

No other agencies will have access to the system.

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.

User roles identify the information and applications a user can access. Following are the roles and access for SF-MFH application.

#	Role	Responsibilities	Access Type	Ability
1	Station Support Staff (Assistant)	1. Inbound Program Comms (information) 2. Inbound Caregiver & Foster Home Program Paperwork System Entry 3. Inbound Veteran Program Paperwork System Entry	Station Level (one station)	Station Level (read & edit) Capability

2	Station Coordinator	1. Outbound Program Comms & Intake (information & VHA Consults/Referrals) 2. Outbound Caregiver & Foster Home Program Visits and Management 3. Outbound Veteran Visits and Management	Station Level (one station)	Station Level (read & edit) Capability
3	Supervisor	1. Overlook multiple MFH stations activity 2. Assist multiple MFH stations with blockers 3. Governance over multi station case types 4. Reviews multi station insights & reports	Multi Station Level (more than one station)	Multi Station Level (read & edit) Capability
4	National Officer	1. Reviews program wide data, insights, & reports 2. Governance over specific case types	Program wide Level (All stations)	All Station Level (read only) Capability
5	SF Admin	1. User Setup 2. System Case/ticket management	Program wide Level (All stations)	All Station Level (read & edit) Capability

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.

Yes, VA contract employee from the DTC and possibly from the contract being managed by the Contracting Officer's Representative (COR) have access to SF-MFH. Access is verified through the (COR) and other VA supervisory/ administrative personnel before contractors are granted to any VA system.

Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS). The Office of Contract Review operates under a reimbursable agreement with VA's Office of Acquisition, Logistics and Construction (OALC) to provide pre-award, post-award, and other requested reviews of vendors' proposals and contracts.

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.

Initial and annual Security Awareness Training includes security best practices, threat recognition, privacy, compliance and policy requirements, and reporting obligations. Upon completion of training, personnel must complete a security and privacy quiz with a passing score. All required VA privacy training must be completed in TMS prior to the user being provisioned.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 04/05/2023
3. *The Authorization Status:* Active
4. *The Authorization Date:* 08/07/2023
5. *The Authorization Termination Date:* 08/06/2025
6. *The Risk Review Completion Date:* 08/07/2023
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 No or In Process, provide your ***Initial Operating Capability (IOC) date.***

In-process with Initial Operating Capability (IOC) date of 08/15/2024.

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)*

Yes, SF-MFH utilizes Salesforce Gov Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This is under the contract: “Salesforce Subscription Licenses, Maintenance and Support”, Contract Number: NNG15SD27B. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus.

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.*

Yes, VA has full ownership of the PII that will be used in the system.
Contract agreement “Salesforce Subscription Licenses, Maintenance and Support”, Contract Number: NNG15SD27B.

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.

No ancillary data is collected by this system.

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, it is, as VA is utilizing Salesforce Government Cloud Plus. Information is only shared internally.

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).*

This system will not be utilizing 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 provided in this Privacy Impact Assessment is true and accurate.

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2024.06.18 08:11:01 -04'00'

Privacy Officer, Dennis Lahl

JAMES BORING Digitally signed by JAMES BORING
Date: 2024.06.20 09:14:29 -04'00'

Information Systems Security Officer, James Boring

MICHAEL DOMANSKI Digitally signed by MICHAEL DOMANSKI
Date: 2024.06.18 14:21:09 -04'00'

Information Systems Owner, Michael Domanski

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).

Notice of Privacy Practices (NOPP)

Department of Veterans Affairs Veterans Health Administration Notice of Privacy Practices (Effective Date September 30, 2019)

Salesforce Security Guide

VA VHA Directive 1605.01 Privacy and Release of Information

VA System of Record Notice (VA SORN) Community Residential Care and Medical Foster Home Programs VA, SORN 142VA10 (July 28, 2023) https://www.govinfo.gov/conten/pkg/FR-2023-07028/2023-16020.pdf

VA System of Record Notice (VA SORN) Caregiver Support Program – Caregiver Record Management Application (CARMA), SORN 197VA10 (April 9, 2021) https://www.govinfo.gov/content/pkg/FR-2021-04-09/pdf/2021-07310.pdf

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/

VHA Publications:
https://www.va.gov/vhapublications/publications.cfm?Pub=2

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