Privacy Impact Assessment for the VA IT System called:

Salesforce – Status Query Response and Exchange System (SQUARES)

Veterans’ Health Administration

Homeless Program Office

Staff Sergeant Parker Gordon Fox Suicide Prevention

eMASS ID #1975

Date PIA submitted for review:

6/11/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	James C. Boring	James.Boring@va.gov	202-842-2000 x4613
Information System Owner	Mike Domanski	Michael.Domanski@va.gov	727-595-7291

Abstract

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

Salesforce (SF) – Status Query Response and Exchange System (SQUARES) is the redesign of the SQUARES portal and migration into the VAEMCC SF org from the VAPM SF org. SQUARES will enable users to quickly retrieve reliable information about the Veteran status and eligibility for programs including, but not limited to Veteran Status and Veteran Health Administration (VHA) healthcare, VA Homeless, VA Homeless Legal Services (LSV-H), and for the Staff Sergeant Parker Gordon Fox Suicide Prevention Grant Program (SSG Fox SPGP). Representatives can enter unique identifiers, such as the Veteran's name, date of birth (DOB), gender and social security number (SSN) to obtain program status and eligibility information. SQUARES is administered by the Department of Veterans Affairs (VA) VHA Homeless Program Office (HPO) to enable VA homeless program staff and external service providers to retrieve Veteran status, VA program eligibility, and VHA enrollment status. SQUARES will be used by VA staff, and by organizations receiving VA homeless program grant funding--Supportive Services for Veterans Families (SSVF), Grant and Per Diem (GPD), Legal Services (LSV), Contracted Emergency Residential Service (CER), Housing Urban Development-VA Supportive Housing (HUDVASH), HUD Continuum of Care (CoC) and community-based homeless services organizations. SQUARES runs on the Salesforce platform and provides single or batch Veteran status and user lifecycle management including application, approval, notification, etc. SQUARES is integrated with the Master Person Index - Enhanced (MPI-e), VHA Eligibility, ID.Me. SQUARES will provide users with identity traits of the matched individual(s) found in VA databases, which allow users to assess whether the match is accurate through a Veteran status indicator that identifies key limits for Homeless program, Homeless Legal Services, SSG Fox SPGP, Veteran Status and VHA eligibility. The application will also allow users to submit bulk queries of Veterans rather than submitting everyone separately. SQUARES includes a robust user approval system to properly control the disclosure of a wider set of data fields within the enhancement. SSG Fox SPGP grantees can complete single searches only. In 2023, the SSG Fox SPGP was integrated into SQUARES, allowing SSG Fox SPGP grant organizations to confirm Veteran eligibility for this suicide prevention grant program. SQUARES is integrated with the Master Person Index - Enhanced (MPI-e), VHA Eligibility, and ID.Me.

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?*
SQUARES is owned by the Homeless Program and Staff Sargent Gordon Parker Fox Suicide Prevention Programs in VHA.

B. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
SQUARES is a VA web application that provides VA employees and external service organizations with reliable, detailed information about Veteran eligibility. Users submit identity attributes for individuals (name, date of birth, social security number, gender) and SQUARES returns information regarding their Veteran status and VHA enrollment and eligibility as well as VA program eligibility including, but not limited to VA Homeless, Homeless Legal Services (LSV-H), and SSG Fox SPGP for grantee partner organizations only. The tool facilitates quick and simple access to care for homeless and at-risk Veterans. SQUARES directly supports the HPO's mission of ending Veteran homelessness and the mission of reducing Veteran Suicide because of its unique ability to empower external organizations with the use of Veteran data.

C. *Who is the owner or control of the IT system or project?*
SQUARES is operated by Homeless Program Office & Suicide Prevention - VHA.

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 IT system is owned by the VHA HPO and is controlled under the Salesforce Authority to Operate (ATO), Affected individuals are VA employees and external organizations known as users. The expected number of individuals internal VA users is approximately 1,350, while the expected number of external partner organization users is 6,500 which includes both active and inactive legacy 2.0 users.

E. *What is a general description of the information in the IT system and the purpose for collecting this information?*
The information in the system is the Name, work email and organization to which the user is affiliated. The purpose of this information is to provide access to the system to determine eligibility.

F. *What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.*
SQUARES internal pass through is Salesforce to the API Middle ware. This is read only the system does not store or edit.

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?*

SQUARES is only operated on one website but is operated at hundreds of physical sites across the country. The secure, 2 factor authenticated access to the system is present at all physical sites where SQUARES is used. PII is maintained consistently within the internal back-end data source where it was temporarily pulled from in SQUARES, but not stored. All sites utilize control outlined in the Data Use Agreement for the allowable usage of PII.
The Cloud Service Provider for SQUARES is Salesforce Government Cloud Plus -Enterprise (SFGCP-E).

3. Legal Authority and SORN

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

SQUARES is housed on the Salesforce platform, which has an Authority to Operate (ATO) at the Digital Transformation Center (DTC) at Electronically pulled from VHA via the E&E web service. System of record number (SORN#): 121VA10 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: 38 U.S.C 501
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.

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?*

SORN 121VA10 requires an amendment to include the name, phone number, address, and email of non-VA employee community partners who will have profiles created for access to the system.

4. System Changes

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

Completion of this PIA will not result in significant business process changes and the application solution for SQUARES will support current business processes.

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

The system also uses cloud technology which is covered in the SORN

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:

- First//Middle/Last Name/Suffix
- Aliases, if any known
- Cadency
- Date of Birth
- Date of Death
- Death Indicator
- Social Security Number
- Gender
- VA ID
- Service Number
- Service Branch
- Personnel Category Code

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

- Character of Discharge (whether served honorably or otherwise, per active-duty period)
- Separation Code
- Enter on Duty Date(s) to active duty in the military services
- Date(s) of Discharge from active duty in the military services
- Non-Pay Days
- Pay Plan Paygrade
- Electronic Data Interchange Person Identifier (EDIPI)
- Narrative Reason for Separation (per active-duty period)
- Veteran Eligibility
- Veteran Type (Title 38 Status)

PII Mapping of Components (Servers/Database)
Salesforce – Status Query Response and Exchange System consists of 4 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 – Status Query Response and Exchange System consists** 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.

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
VA Salesforce Government Cloud Plus (SFGCP), via Business Partner Extranet (BPE) Connection. va.my.salesforce.com	YES	NO	Veterans Data Elements include: -First//Middle/Last -Name/Suffix -Date of Birth -Social Security -Number -Gender -Veteran Eligibility	Determine Eligibility for Benefit	System SSN is masked
Salesforce GovCloud (FedRAMP)	YES	NO	-Veteran Type (Title 38 Status) -Character of Discharge (whether served honorably or otherwise, per active-duty period) -Narrative Reason for Separation, per active duty period	Determine Eligibility for Benefit	System SSN is masked.
Beneficiary Identification Records Locator Subsystem:	YES	NO	-First//Middle/Last Name/Suffix -Aliases, if any known -Cadency -Date of Birth	Determine Eligibility for Benefit	System SSN is masked.

Veterans Health Information System and Technology Architecture/ Administrative Data Repository			-Date of Death • Death Indicator • Social Security Number • Gender • VA ID • Service Number • Service Branch • Personnel Category Code • Character of Discharge (whether served honorably or otherwise, per active-duty period) • Separation Code • Enter on Duty Date(s) to active duty in the military services • Date(s) of Discharge from active duty in the military services • Non-Pay Days • Pay Plan Paygrade		
United States Veterans/Social Security Administration Verification va.my.salesforce.com Salesforce GovCloud (FedRAMP)	YES	NO	-Death Indicator -Social Security -Number -Gender -VA ID -Service Number -Service Branch -Personnel -Category Code Character of Discharge (whether served honorably or otherwise, per active-duty period) -Separation Code -Enter on Duty Date(s) to active duty in the military services -Date(s) of Discharge from active duty in the military services -Non-Pay Days -Pay Plan Paygrade	Determine Eligibility for Benefit	System SSN is masked.

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?

Data is returned from U.S. Department of Defense Identity Repository and VA Profile

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.
Data only comes from Master Veteran Index (MVI), Electronic Service Record (ESR), and VAPROFILE VA resources

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
There are two types of information used in the system, some of which overlaps. Input information is collected from the client (i.e., the Veteran). Output information is required to determine if the client is a verified Veteran, and to determine if their service qualifies them for programs including, but not limited to Homeless, Homeless Legal Services (LSV-H), Suicide Prevention (SSG Fox SPGP), and Veteran Status and Veteran Healthcare (VHA). The system does not create information or store it in any form. VA data sources: Beneficiary Identification Records Locator Subsystem, Veterans Health Information System and Technology Architecture/ Administrative Data Repository, United States Veterans/Social Security Administration Verification

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?
Information is collected verbally/physically and input into form within system. Data points collected can include: First Name, Last Name, DOB, Gender, SSN.

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?
No data is collected on the web 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.
SQUARES call to the data source used both attended and non-attended accuracy checks, both are completed with match scores and high-fidelity matches.

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?
SQUARES call to the data source used both attended and non-attended accuracy checks, both are completed with match scores and high-fidelity matches.

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

SORN 121VA10 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. Authority for maintenance of the system: 38 U.S.C 501. This SORN is being amended to include VA partner information needed to provide access to the system.

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

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: The information displayed on the screen to the end user is relevant for determining an eligibility status for the Veteran in question. The end user of the system does collect information directly from the individual for purposes of running a search to verify their identity and service information, not for any medical purposes. The PII that is temporarily displayed belongs to official VA data sources, therefore it is checked for accuracy there. One risk is that a user could do a screen print and save it or print it

Mitigation: Access Controls – 2 factor authentications, signed agreement with VA on data usage (DUA), permission-based access on need-to-know basis, Encryption in transit

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.

SQUARES operates under Veteran Experience Office Eligibility & Enrollment and VHA Homeless Program Office to support the mission of ending Veteran Homelessness and reducing Veteran Suicide Users utilize search data from return to search to determine a person's Veteran status, and their eligibility for VA homeless programs, VHA Healthcare and SSG Fox SPGP. Data elements are split up into two categories, inputs, and outputs. They and are used in the following ways, by both internal VA users and external Community users, within the SQUARES Community

PII/PHI Data Element	Internal Use	External Use
Input Data: First/Last Name, DOB, SSN, Gender	Use: any combination of the data elements are entered to execute an Advanced Search to find a Veteran Output data: Alias, Cadency, Date of Death, Death Indicator, VA ID, Service Number, Service, Component, Character of Service, Separation Code, Enter on Duty Date(s), Release from Active Duty Date(s), Non Pay Days, Pay Plan Pay grade Note: There are different combinations of the above 14 fields that can help the end user make the Veteran status and VA homeless services, VHA Healthcare and/or SSG Fox SPG Eligibility determinations	Use: any combination of the data elements are entered to execute an Advanced Search to find a Veteran Output data: Alias, Cadency, Date of Death, Death Indicator, VA ID, Service Number, Service, Component, Character of Service, Separation Code, Enter on Duty Date(s), Release from Active Duty Date(s), Non Pay Days, Pay Plan Pay grade Note: There are different combinations of the above 14 fields that can help the end user make the Veteran status and VA homeless services, VHA Healthcare and/or SSG Fox SPG Eligibility determinations

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?

VA Operations employees will have the ability to run reports on Veterans Search information with the following data attributes of the search performed and program eligibilities of veterans and partner organization users.

- Partner Organization, City, and State.
- Veteran Search Number
- Associated VA Medical Center
- Homeless, Legal Services, and Suicide Prevention Program Eligibility Codes
- VHA Eligibility Status
- VHA Enrollment Status
- Veteran Status
- Veteran First Name
- Veteran Last Name
- Gender
- Search Date
- Search Status
- Partner Username
- Partner User
- User Type (Internal or External)

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.

SQUARES do not make unutilized information discoverable, data in transit is protected via a secure connection to the API/middleware that passes data from the source to the application, and encryption in transit. Data at rest is protected via Access Controls and an auto-clear process. The system does not retain data, however Social Security Numbers that are displayed on screen are partially masked to only display the last 4 digits. The SSN search field also auto-hides characters as they're typed in

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 protected via a secure connection to the API/middleware that passes data from the source to the application, and encryption in transit. Data at rest is protected via Access Controls and an auto-clear process. The system does not retain data, however Social Security Numbers that are displayed on screen are partially hidden to only display the last 4 digits. The SSN search field also auto-hides characters as they're typed in.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
The system does not retain data, however Social Security Numbers that are displayed on screen are partially masked to only display the last 4 digits. The SSN search field also auto-hides characters as they're typed in. Two-factor authentication; SSN masking; Salesforce Shield Encryption with AES 256-bit encryption at rest; SQUARES utilizes MPI for the identity trait-based search. MPI returns the DoD EDI Person Identifier (EDI PI) and that identifier, not SSN, is used for retrieval of military service data needed to determine benefit eligibility.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
All data is not retained and read only. When the session is close the data is removed

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? Every user is required to have an ID-Me account or be a VA Employee.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? Access controls are in place to ensure that only approved users can access the SQUARES search features. There is system training that users are required to complete before applying for access with manager approval. There are reminders throughout the system reminding users not to transmit PII without encryption.

2.4c Does access require manager approval?
Yes- The system admin approves all user access

2.4d Is access to the PII being monitored, tracked, or recorded?
The application uses Server Access logging i.e., Event logging on the server

2.4e Who is responsible for assuring safeguards for the PII?
SQUARES Admin role.

Section 3. Retention of Information

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

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is ***retained*** *by the system.*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal
The data element retained is just the user access log information. It is stored in the Salesforce system indefinity even after an account is marked disabled.

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.*
All user accounts are stored in the Salesforce system encrypted, once an account is marked de-active the account stays on file. The current SORN is being updated. We will update this section when it is completed and make system changes if necessary.

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?

Yes- approved.

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

Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule (GRS), 5.2 Transitory and Intermediary Records, item 020. GRS 5.2: https://www.energy.gov/sites/default/files/2023-01/grs%205.2%20Transitory%20and%20Intermediary%20Records%20Schedule%20trs31%20DOE%20trs05.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.

Search results are auto cleared when navigating to other pages within system. Session management auto-clears results and logs users out after 15 minutes of inactivity.

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 only used for testing in a pre-PROD environment by administrative use only, with Single Sign On (SSO) access controls.

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: Data is not retained, and search results are auto cleared when logging out, or when navigating to a new page within the system. The user could make a screen capture and save or print

Mitigation: Access to search data is restricted to only those users with a need to know. Search data is auto cleared by the system

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***
Office of Veterans Health Administration (VHA) Enrollment and Eligibility Records	Critical web service connection to MPI-E API to identify and return Veteran profile matches with SSC Eligibility Description, VHA Eligibility, VHA Enrollment, and Military Status.	SSN, DOB, Name, Sex, Death Date, Death Indicator	Electronically pulled from VHA via the E&E web service. System of record number (SORN#): 147VA10. Data is returned for specifically queried individuals
Office of Veterans Health Administration (VHA) VA Identity	Critical data source connection to transform SSN into an	SSN, DOB, Name, Sex, Death Date, Death Indicator	Electronically pulled from VHA. System of record number

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***
and Service Services Master Person Index (MPI)	EDIPI for a data return in the advanced search		(SORN#): 121VA10. MPI records are returned for specifically queried individuals via MPI's search services
Office of the Secretary of Veterans Affairs / Office of Veterans Experience Veterans Affairs / Department of Defense Identity Repository (VADIR)	Critical data source connection to return data in the advanced search. (See above)	SSN, DOB, Name, Sex, Death Date, Death Indicator	Electronically pulled from VHA via eMIS, a web service maintained by VIERS. System of record number (SORN#): 138VA005Q. Data is returned for specifically queried individuals.

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: SQUARES call to the data source used both attended and non-attended accuracy checks, both are completed with match scores and high-fidelity matches

Mitigation: Access Controls – 2 factor authentication, signed agreement with VA on data usage (DUA), permission-based access on need-to-know basis, Encryption in transit

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***
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 are inherent minor risks with sharing information between colleagues within an external organization.

Mitigation: Access Controls – 2 factor authentication, signed agreement with VA on data usage (DUA), permission-based access on need-to-know basis, Encryption in transit

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.

The VHA Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.

Notice is also provided in the Federal Register with the publication of the SORN 121VA10 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. This SORN is being amended to include VA partner information that is collected. This Privacy Impact Assessment (PIA) also serves as notice 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."

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

Notices was provides as indicted in 6.1a above

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 VHA Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.

Notice is also provided in the Federal Register with the publication of SORN 121VA10 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. This SORN is being amended to include VA partner information needed to provide access to the system.

This Privacy Impact Assessment (PIA) also serves as notice 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."

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.
Individuals (Veterans) have the right to decline to provide personal information. If so, they cannot be serviced. There is no "denial of service attached."

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.
Information is used, accessed, and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR. Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed, and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

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?
Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:
Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.
Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, the NOPP is also available at all VHA medical centers from the facility Privacy Officer.

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

SORN 121VA10 "National Patient Databases-VA" https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above or write or visit the VA facility location where they normally receive their care. A request for access to records must contain the requester's full name, address and telephone number, be signed by the requester and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

The information used by SQUARES is obtained from other systems within VA. There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the My HealtheVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at http://www.myhealth.va.gov/index.html.

Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) Office. VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access. VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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)?

N/A – The system is not exempt from the Privacy Act.

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

N/A – The system is not exempt from the Privacy Act.

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

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

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information.

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal.
- File a “Statement of Disagreement”
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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. ***<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3. In addition to the formal procedures discussed in question 7.2 to request changes to one's health record.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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 considering 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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:

<u>Privacy Risk:</u> Because SQUARES is not the system of record for Veteran information, nor does it correct erroneous information, there is the propensity for incorrect information remain that way and keep the Veteran from accessing services

<u>Mitigation:</u> An end user can reach out to their assigned VA Medical Center (VAMC) for the correct process to address data inaccuracies. Veterans' area able to request the correction of the inaccurate information identified in their record via the process identified in question 7.2 above.

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?
To receive access to SQUARES there are several layers:

1) Must complete the User Access Data Agreement
2) Must have an ID-ME Account or be VA Approved
3) Must be approved be an administrator.

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?
SQUARES don't share PII information with other agencies. And user access is approved only by the SQUARES administrator that is a VA Employee

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.
All users have read only access. SQUARES users are External (Manager), External (Standard Users) SQUARES Administrators (only VA Employee)

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 contractors have access to the system. Their only access to PII is in the Staging (pre-PROD) for testing purposes.
All VA contractors complete a security and awareness training during the onboarding process, prior to receiving system access.

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.

There is specified SQUARES training for end users, required before they can apply for access.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* May 19, 2023
3. *The Authorization Status:* Approved
4. *The Authorization Date:* June 1, 2023
5. *The Authorization Termination Date:* June 1, 2024
6. *The Risk Review Completion Date:* June 1, 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.***

Salesforce has an approved security plan as 24 Feb 2021 and a full ATO, through October 2024. SQUARES current has a moderate Data Security Categorization.

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, Salesforce GovCloud has FedRAMP authorization. And PaaS. PaaS products are hardware and software tools from third-party software companies that equip VA teams with the building blocks to create their own customized applications (with the help of a qualified developer). The programs created can be for local use only, or scaled up for deployment throughout VA.

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.*

The Salesforce application (SQUARES) does not have ownership over any PII data. Contract number: T4NG-0534 | VA-20-00037251

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.

Meta data and audit trails are only captured if specifically set to do so on the system's backend

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.

Meta data and audit trails are only captured if specifically set to do so on the system's backend

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 goal of SQUARES is to allow non-VA and VA providers to quickly determine homeless individuals' eligibility for Veteran programs., VA Grantees associated with Supportive Services for Veteran Families (SSVF), Grant and Per Diem (GPD), Contract Emergency Residential Services (CERS) and Staff Sergeant Parker Gordon Fox Suicide Prevention Grant Program (SSG Fox SPGP) may quickly determine individuals' eligibility for Veteran homeless and suicide prevention grant programs. In addition, HUD VASH Identity attributes (Name, Date of Birth, Social Security Number, and Gender) are entered using the single or bulk search features of SQUARES. SQUARES invokes the VA Master Person Index (MPI) web services using the identity attributes; if the person matches to a known individual, MPI returns the DoD Electronic Data Interchange Person Identifier (EDI PI) and the authoritative identity data for the individual. This EDI PI is then used to invoke the enterprise Military Information Service (eMIS) which queries the VA/DoD Identity Repository (VADIR) to retrieve the individual's military history and return it to SQUARES, where it is evaluated to determine potential eligibility for VA programs. The application is being hosted by the FedRAMP approved Salesforce GovCloud.

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.

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2024.07.01 09:01:43 -07'00'

Privacy Officer, Phillip Cauthers

JAMES BORING

Digitally signed by JAMES BORING
Date: 2024.07.01 10:12:20 -04'00'

Information System Security Officer, Jim Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2024.06.27 13:43:19 -04'00'

Information System Owner, Mike 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).

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

SORN 121VA10 “National Patient Databases-VA”: https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.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/

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

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