Privacy Impact Assessment for the VA IT System called:

Juvare Federal Cloud-Enterprise

Veterans Health Administration (VHA)

Office Of Emergency Management (OEM)

eMASS ID: 2013

Date PIA submitted for review:

11/20/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Philip.cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Jose Diaz	Jose.Diaz4@va.gov	312-980-4215
Information System Owner	Rob Maas	Rob.maas@va.gov	352-672-3028

Abstract

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

The purpose of the Juvare Federal Cloud (JFC) system is to provide the Veterans Health Administration (VHA) Office of Emergency Management (OEM) with an information technology (IT) solution to assist in preparing for, responding to and managing disasters and incidents affecting both the VHA and the nation.

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?*
The IT system name and the name of the program office that owns the IT system. Juvare Federal Cloud (JFC) is Software as a Service (SaaS) that will be controlled by the VHA Office of Emergency Management.

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

JFC will bolster the capability of the OEM to provide situational awareness, improve collaboration at all levels, coordinate and employ response resources and make key leader decisions much faster. This capability will allow the VHA to better prepare for and respond to multiple incidents occurring at the same time, such as a hurricane or earthquake response during the pandemic which will ensure the continuum of healthcare, protect our facilities and save lives.

Juvare, LLC ("Juvare") has established Juvare Exchange Government Cloud platform using automation to quickly replicate the environment. This solution is referred to as the Juvare Federal Cloud (JFC). JFC is a solution that encompasses a collection of applications available for use by clients (external parties). The Juvare technical team configures all applications to the clients (external parties) specific/unique specifications. The applications included within the authorizations are as follows:

- **Juvare Exchange (JX)(v1.39.2)** – This application serves as a data warehouse that houses copies of all application data. This application processes information in the background and uses the following URI base paths (dynamic—each Federal Agency Organization are issued their own second-level domain (SLD) in the FQDN:

  - /io/portal
  - /normalizer
  - /input

- /webeoc-push
- /external

• **Platform Service (v1.16.4)** - Configuration Service is used to configure access between client facing Juvare products (example, WebEOC) and Juvare internal services (Juvare Exchange, Alert Service, Notify Service, etc…). The main purpose of Configuration Service is to have all Juvare services configurations outside client facing product (example WebEOC).

- /product/platform/api
- /app

• **WebEOC (v9.15)** – Is a Crisis information management system. This application is specifically used by clients (external parties). When deployed, there will be multiple clients of WebEOC; configurations of which are customized by the client and provided to Juvare for creation. Once all configurations have been received the use of the application is tuned over to the client for use and this application uses the following URI base paths (dynamic—each Federal Agency Organization are issued their own second-level domain (SLD) in the FQDN:

- /eoc9/api/mobile/rest.svc/
- /eoc9/api/rest.svc/ o /eoc9/api.asmx
- /eoc9/platform/
- /eoc9/api/boards

• **Design Studio (v1.8)**

- Includes Board Studio (v1.8) and Form Studio (v1.8)
- Design Studio is Juvare's designer for WebEOC. Design Studio gives WebEOC administrators drag-and-drop functionality and editing flexibility in building boards.
- Boards are created through the editor by dragging components onto the canvas and specifying component details, such as the label and help text. Once ordered and laid out properly, Design Studio can quickly generate display views, review the table, and if appropriate, create resources.
- The enhanced designer is also a rich board management process that includes creating metadata such as a description, status, and tags. This information helps board organization by clearly defining the purposes they serve
- The following URI base paths are:

    - /publisher
    - /forms-api
    - /studio-api
    - /boards-api
    - /forms/[UUID]

• **Alert Service (v.1.35) / Notify Service (v1.35)** - The Alerts Plug-In is used to connect with WebEOC users, other employees in your organization, and external contacts through dedicated notification channels. These channels include voice and text channels, in addition to webhooks (such as Microsoft Teams and Slack), complement existing email, mobile push, and control panel notifications, to make sure everyone is informed. Notification channels are configured to send notifications on board record creation or update, as well as create recurring or one-time scheduled notifications not related to board records. This application uses the following URI base paths (dynamic—each Federal Agency Organization are issued their own second-level domain (SLD) in the FQDN:

- /control
- /manage
- /twilio/voice p
- /inbox
- /front
- /respond
- /efax/fax
- */aws/email*
- */alert*
- */twilio/sms*
- */pinpointsms*
- */pinpointvoice*
- */r/*
- */ - uses custom dns [name].federal.juvare.us*

The cloud services included within the authorizations are as follows:

• AWS GovCloud
• Microsoft Azure Government
• ServiceNow – Government Community Cloud JFC is a multi-cloud solution for identity providers. The cloud service providers included within the authorizations are as follows:

• AWS AD Connect – Workforce management
• Microsoft Azure AD – Customer/multi-tenancy logins
• Okta – Customer/multi-tenancy logins

Juvare leverages a Cloud Managed Services offering (Ref: JFC Platform Team) that is used to assist with the building of the JFC's platform up through the OS. The JFC Platform Team provides complete management of cloud services from initial provisioning through the entire solution life cycle; including software licensing and configurations for the tools required to manage and monitor the various JFC environments; and the system specific portal provides access into service request, event and incident ticket management systems.

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

Juvare Federal Cloud will be owned by the VHA Office of Emergency Management (OEM) and the Veterans Health Administration (VHA) and controlled by Juvare.

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?*

Across all 4 instances, there will be an estimated 7,660 users ranging from VA employees, Veterans/dependents, and volunteers.

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

At log-in to the system, users will be asked and given an opportunity to input and remediate information exclusive to their: name, specialty, VA profession, work phone number, and work email address. The purpose of collecting the information is for the purpose of registering individuals for access to the system.

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

The system will not be conducting any method of information sharing.

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?*

This system is operated across 4 sites: VHA Office of Emergency Management, Office of Performance and Quality at the Erie VA Medical Center, VISN 16 Emergency Management, and the VHA Chief of Staff's Office. Each site has its own instance of the system but using the same controls at each. PII is not shared across sites:

PR-00525: The purpose of the Juvare Federal Cloud (JFC) system is to provide the Veterans Health Administration (VHA) Office of Emergency Management (OEM) with an information technology (IT) solution to assist in preparing for, responding to and managing disasters and incidents affecting both the VHA and the nation. JFC will bolster the capability of the OEM to provide situational awareness, improve collaboration at all levels, coordinate and employ response resources and make key leader decisions much faster. This capability will allow the VHA to better prepare for and respond to multiple incidents occurring at the same time, such as a hurricane or earthquake response during the pandemic which will ensure the continuum of healthcare, protect our facilities and save lives. The data security categorization that has been provided to us by the information system security engineer assigned to this system has returned to us at a high watermark.

PR-01550: Juvare Federal Cloud (JFC) will be used by the Office of Performance and Quality (OPQ) and the Erie VA Medical Center (VAMC) as an emergency management notification system for their employees, volunteers, and veterans, as well as to keep a staff record and conduct surveys for environmental sustainability.

PR-02163: Juvare Federal Cloud (JFC) will be used by VISN 16 Emergency Management as an emergency management notification system for employees and veterans within VISN 16, allowing users to receive notifications in emergency situations to promote safety.

PR-03311: Juvare Federal Cloud (JFC) will be used by the VHA Chief of Staff's Office as an emergency management notification system that allows for the ability to reach veterans in adverse situations.

3. Legal Authority and SORN

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

VHA Office of Emergency Management is the requesting office for this system. A Privacy Act SORN is not applicable to this system as the data collected is not searchable by an individual's unique personal identifier. The purpose of the system is to enhance emergency management communication and decision making. Below is a comprehensive list of directives that the requesting office operates under:
a. The Homeland Security Act of 2002, PL §§107-296, 6 U.S.C.101-557, November 25, 2002.
b. Department of Veterans Affairs Emergency Preparedness Act of 2002, PL 107-287, U.S.C §1785 (2003)
c. Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended, 42 U.S.C. §5121, et seq.
d. Public Law 97-174, May 4, 1982, as amended, Title 38 USC §8111A "VA and DOD Health Resources Sharing and Emergency Operations Act".
e. Homeland Security Presidential Directive/HSPD-5, February 28, 2003.
f. National Security Presidential Directive-51/Homeland Security Presidential Directive-20, National Continuity Policy, May 9, 2007.
g. Presidential Policy Directive 8 (PPD-8), March 30, 2011.
h. National Communications System Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, July 25, 2007. (Classified Document)
i. National Response Framework, January 2008.
j. National Incident Management System (NIMS), December 2008.
k. Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements, February 2008.

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?

N/A

4. System Changes

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

The completion of this PIA will not result in circumstances that require changes to business process nor the technology but instead supplement and reinforce them.

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

The completion of this PIA will not result in circumstances that require changes to business process nor the technology but instead supplement and reinforce them.

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

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

☐ 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:

- Specialty
- Profession
- Work Phone Number
- Work Email Address
- Position Title
- Department
- Supervisor Name
- Supervisor VA Work Email Address
- SEC ID
- PIV Number
- Expiration date of PIV Card

PII Mapping of Components (Servers/Database)

Amazon Web Services EC2 consists of an array of key components (databases) based on the geographical location. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Juvare Web EOC 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**
AWS EC2 AWS Fargate Amazon Pinpoint Amazon Aurora PostgreSQL Amazon RDS MS SQL	Yes	Yes	• Name, VA employee specialty, VA employee profession • Work phone	Necessary for log into the system Also necessary for internal directory	Data base is encrypted at rest and at transit. Logged and monitored access to

Amazon S3 Amazon ElastiCache Amazon SES Amazon SQS Amazon ECS Amazon API Gateway Amazon Kinesis Data Streams AWS Lambda Amazon VPC Amazon Connect Amazon MQ			number, Work email address. • Personal mailing and email address, personal phone number • Emergency Contact information, Next of kin • Position Title •Department • Supervisor Name, Supervisor VA Work Email Address • SEC ID, PIV Number, Expiration date of PIV Card		data. Compliant with FedRAMP high controls.

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?

VHA personnel with a role in emergency management will be providing information to be notified by the system in the event of an incident or emergency.

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.

N/A, source is only the individual.

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

N/A

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?

No, Information is being collected directly from the individual/user upon log-in to the system.

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, Information is being collected directly from the individual/user upon log-in to the system.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The process of checking the accuracy of the data will be a user-based action. Upon log-in to the system the user is presented with an opportunity to remediate or remove private information. The information will not be checked against another source or computer for accuracy as it can be audited at log-in.

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?

N/A

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*

VHA Office of Emergency Management is the requesting office for this system. A Privacy Act SORN is not applicable to this system as the data collected is not searchable by an individual's unique personal identifier. The purpose of the system is to enhance emergency management communication and decision making. Below is a comprehensive list of directives that the requesting office operates under:

a. The Homeland Security Act of 2002, PL §§107-296, 6 U.S.C.101-557, November 25, 2002.

b. Department of Veterans Affairs Emergency Preparedness Act of 2002, PL 107-287, U.S.C §1785 (2003)

c. Robert T. Stafford Disaster Relief and Emergency Assistance Act, Public Law 93-288, as amended, 42 U.S.C. §5121, et seq.

d. Public Law 97-174, May 4, 1982, as amended, Title 38 USC §8111A "VA and DOD Health Resources Sharing and Emergency Operations Act".

e. Homeland Security Presidential Directive/HSPD-5, February 28, 2003.

f. National Security Presidential Directive-51/Homeland Security Presidential Directive-20, National Continuity Policy, May 9, 2007.

g. Presidential Policy Directive 8 (PPD-8), March 30, 2011.

h. National Communications System Directive 3-10, Minimum Requirements for Continuity Communications Capabilities, July 25, 2007. (Classified Document)

i. National Response Framework, January 2008.

j. National Incident Management System (NIMS), December 2008.

k. Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity

Program and Requirements, February 2008.

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:

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

The info collected will support the VHA and OEM to prepare and recover from incidences and disasters

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

-Yes

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

-Yes

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

- Yes, information is collected directly from the individual

Follow the format below when entering your risk assessment:

<u>Privacy Risk:</u> By collecting the information previously listed, the system will use this to communicate with its users in the event of an incident or emergency. This information is directly relevant and necessary to accomplish the function of this system and collects this information directly from its users. A potential risk is always breach and if this were to occur, trust with the VA will also be lost.

<u>Mitigation:</u> The process of collecting this information is a self-acting accuracy measure in that the input for it comes straight from the user. It also gives the user the ability to remediate or remove the information at log-in every time. One method of mitigation here is the development of an Incident Response Plan (IRP). Secondly, while the information is in transit it will be encrypted by TLS 1.2 and as the information is at rest it will be encrypted with AWS KMS (FIPS Certificate number 3139). Lastly, in order to gain access to the system, a user must gain predetermined access given by the system administrators.

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.

This information will be used to communicate with the user in the event of an emergency or incident.

Further details allow for the system to pinpoint exactly who is affected by an event and reach out to additional points of contact as needed:

- Name
- VA employee specialty
- VA employee profession
- Work phone number
- Work email address
- Personal mailing and email address
- Personal phone number
- Emergency Contact information
- Next of kin
- Position Title
- Department
- Supervisor Name, Supervisor VA Work Email Address
- SEC ID
- PIV Number
- Expiration date of PIV Card

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?

The system will not be performing any types of data analysis and as such will not be producing any data because of that action.

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 will not be performing any types of data analysis and as such will not be producing any data because of that action.

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?

While the information is in transit it will be encrypted by TLS 1.2 and as the information is at rest it will be encrypted with AWS KMS (FIPS Certificate number 3139).

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

The system will not be collecting, processing, or retaining social security numbers.

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

While the information is in transit it will be encrypted by TLS 1.2 and as the information is at rest it will be encrypted with AWS KMS (FIPS Certificate number 3139).

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII is determined by approval to the system which is only approved by the VA system administrators.

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

There are annual privacy training offered to all VA employees but not specifically regarding JFC.

2.4c Does access require manager approval?

Yes

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

Yes

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

The entire Juvare team is responsible for assuring safeguards for PII but the Juvare Information Security Team is ultimately responsible for compliance. The Juvare team also inherits controls from AWS to further safeguard PII.

Section 3. Retention of Information

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

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is ***retained*** *by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.*

The information that will be retained by the system will be all information types listed in question 1.1.

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.*

Information will be stored in the system for as long as the system is in existence or if the user decides to remove it.

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?

Because JFC records are used by the agency, information will not be deleted and will be maintained indefinitely. The intention for this system is to not remove data as record requests have the potential to be requested any years after an event has occurred.

3.3b Please indicate each records retention schedule, series, and disposition authority? daa-grs-2016-0004_sf115.pdf (archives.gov)

JFC will be utilizing the NARA Retention Schedule DAA-GRS-2016-0004-0001, GENERAL RECORDS SCHEDULE 5.3: Continuity and Emergency Planning Records Item 010. This schedule covers records related to Federal agency internal emergency planning to protect people, government facilities, equipment, and records; safeguard classified or sensitive information; ensure continuity of agency operations in the face of potential natural and man-made disasters; and facilitate timely recovery and return to normal agency operations once the emergency or disaster has passed.

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.

The information upon deletion is cryptographically erased per NIST SP 800-88 guidelines.

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

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

The system does not engage in usages such as those listed above and as such eliminates any risk associated to them.

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 deleted from the program unless the user removes it and when it is removed it is cryptographically deleted per NIST SP 800-88 guidelines. The system only retains information needed to perform its critical functions. A potential risk associated with retention at this duration is that the system administrator may remove data unintentionally by accidental removal.

Mitigation: There is a line included before the removal of data by the user or by the administrator confirming deletion before it happens. At rest before deletion, the data is encrypted by AWS KMS (FIPS Certificate number 3139). The information upon deletion, will be cryptographically erased from the system per NIST SP 800-88 guidelines.

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 , and UL-1, Internal Use.

Data Shared with Internal Organizations

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

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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:

<u>Privacy Risk:</u> N/A

<u>Mitigation:</u> N/A

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***
ORAU (Oak Ridge Associated Universities)	To provide status and operational capabilities of medical centers and to identify volunteers to support disaster response.	Name, work email, work phone number, profession, specialty	The VHA Office of Emergency Management has an established contract with ORAU covering their information sharing agreement.	SSL/TLS 1.2

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> One of the associated risks with sharing information outside the department is the possibility of a breach.

<u>Mitigation:</u> The mitigation variables preventing a breach is a contract that all stakeholders involved adhere to maintaining the security of the system. During the authorization process there will also be a incident response plan so that in the event of an unlikely breach all parties will have designated responsibilities in responding.

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.

USG Warning and Consent Banner

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use. By using this IS (which includes any device attached to this IS), you consent to the following conditions:
• The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
• The USG may inspect and seize data stored on this IS at any time.
• Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
• This IS includes security measures (e.g., authentication and access controls) to protect USG interests-not for your personal benefit or privacy.
• Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications or work product related to personal representation or services by attorneys, psychotherapists, clergy, and their assistants. Such communications and work products are private and confidential. See User Agreement for details.

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

Notice is provided via a web based warning screen they cannot be bypassed.*Enter Major Application name here.*

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.

Data is entered by the individual so the web based warning screen they cannot bypass serves as this notice.

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

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

The system does provide the user with an opportunity to decline providing information. If the user chooses to decline this offering the user would not be able to create an account and thus not have access to the system.

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.

> The choice for compliance in use of specific information is not explicit to the user. The concurrence from the individual is binary in that if the user inputs information that will be considered consent and if the individual does not provide information that will be regarded as a decline of use.

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: The user enters their own information into the system. The user is not given any notice before they are asked to provide information. If this opportunity was not provided to the individual there is a potential risk that there may be a reduced visibility to the user as to the accuracy of the data.

Mitigation: The individual is presented with an opportunity upon log-in to the system to edit or remove information as they choose. This PIA also serves as a notice to the public that the system exists, what information is collected, and how it is used.

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.***

Users have the opportunity to access the information they have provided to the system when they are logged into the system.

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)?

Information in the system is not accessed using an individual's unique identifiers so a Privacy Act System of Record does not apply to the system.

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?

Users have the opportunity to amend their information when they are log into the system. The Juvare Privacy Policy also specifies that questions regarding the Privacy Policy or requests for changes to any personally identifiable information can be referred to compliance@juvare.com or call 866-200- 0165.

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.

Users have the opportunity to amend their information when they are log into the system.

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.

At log-in, users will be given an opportunity to amend their information. The Juvare Privacy Policy also specifies that questions regarding the Privacy Policy or requests for changes to any personally identifiable information can be referred to compliance@juvare.com or call 866-200-0165.

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.

Please see the response to question 7.3 above.

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 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:
<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> Individual users may have inaccurate data if entered incorrectly the first time or data changes at any point in the future.

<u>Mitigation:</u> Individual users are entering their own information and have control over the information with the ability to delete or edit in the future. Juvare may also be contacted directly to request changes to a user's information.

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?

Access to the system will be documented by an identity solution that integrates with VA (SAML). Users are granted access by administrators, 3 people at Head Quarters and one at Juvare (there is no access permission given by Juvare). Administrators identify positions previous to granting access to those identified users.

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?

N/A

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 – The most common type of account; it does not have administrator permissions. **Full Administrator** – This account gives the user full access to the system and administrative tasks; allows one to create and modify any type of user account. Partial **Administrator** – This type of account offers partial administrative permissions. Partial administrators are assigned one or more admin profiles that grant limited access to specific administrative functions.
Sub-administrator – Full administrators can assign the sub-administrator role to users in order to distribute some of the user management workload. The full administrator assigns the users and positions that the sub-administrator can manage. The sub-administrator can manage assigned accounts and run a limited number of reports for this subset of users and positions. Sub-administrators can also create additional user accounts as needed and assign and modify position assignments.
Service – An account type designed for use with Dual Commit, WebEOC® Fusion, or the API, it cannot be used to log in to WebEOC.
Service as Administrator – In addition to having the same properties as the Service account, this account additionally allows users to perform the administrative API functions.

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.*

VA contractors will not have access to this system. Vendor is only contractor that will have access and an NDA is included in the contract.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

General training is given to VA employees by the VA on how to handle PII/PHI but this training is not specific to the JFC system. Juvare performs initial privacy and security awareness training upon hire and ongoing refresher training at least annually.

Initial Training:

1 Security Awareness Fundamentals
2. Preventing Workplace Harassment for Employees
3. Privacy Series: Protecting Personal Information - Security & Safeguards
4. Understanding and Protecting PII
5. Juvare Acceptable Use Policy
6. Juvare Clear Desk Clear Screen Policy
7. Juvare Standards of Business Ethics and Conduct
8. Juvare Policies & Standards on Confluence

Refresher Training:

1. Understanding and Protecting PII
2. Privacy Series: Protecting Personal Information - Security & Safeguards
3. Ethics and Code of Conduct
4. Juvare Standards of Business Ethics and Conduct
5. Preventing Workplace Harassment for Employees

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

8.4a If Yes, provide:

1. *The Security Plan Status: Complete*
2. *The System Security Plan Status Date: 11/10/2023*
3. *The Authorization Status: Authorized*
4. *The Authorization Date: 08/05/2023*
5. *The Authorization Termination Date: 09/04/2025*

6. The Risk Review Completion Date: 09/17/2023
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH): High

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.***

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)*

The system uses cloud technology as defined by NIST 800-145. It is a commercially operated SaaS that is hosted outside the VA in AWS GovCloud. It is in the process of attaining a FedRAMP agency authorization to operate. This system categorizes as a SaaS solution.

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 VA is going to be sole owner of the data. Per contract # NNG15SD27B, "Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1)."

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

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

The Contractor will collect ancillary data to meter and charge for consumption of resources, logs and audit trails. Contractor will also collect metadata that is generated and accumulated within the cloud environment for the purposes of performance monitoring.

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.

As part of the cloud provider's contract, "All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this Product Description."

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 is not taking advantage of RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

PHILLIP
CAUTHERS

Digitally signed by PHILLIP
CAUTHERS
Date: 2024.11.26 10:54:50 -08'00'

Privacy Officer, Phillip Cauthers

JOSE DIAZ

Digitally signed by JOSE DIAZ
Date: 2024.12.02 09:03:43
-06'00'

Information System Security Officer, Jose Diaz

ROBERT MAAS

Digitally signed by ROBERT
MAAS
Date: 2024.12.02 10:52:41 -05'00'

Information System Owner, Rob Maas

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).

Pop-up notice from Juvare referred to in section 6.1a above.

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