SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

VA HANDBOOK 6508.1: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," July 2015, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=810&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

New ORH Management and Analysis Database (NOMAD)

Office of Rural Health (ORH)

Date PIA submitted for review:

4/1/2022

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	julie.drake@va.gov	202-632-8431
Information System Security Officer (ISSO)	James Boring	james.boring@va.gov	215-842-2000
Information System Owner	Michael Domanski	michael.domanski@va.gov	727-595-7291

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

NOMAD is a new system to manage the entire lifecycle of ORH-funded initiatives aimed at increasing access to care for the 2.8 million rural Veterans enrolled in the VA health care system. The goal of NOMAD is to create a single environment for tracking all ORH funded programs and projects – from budget to outcomes including:

- Program information, funding details, and operational costs
- Project information, budget details, approvals, and measures

Congress established the Veterans Health Administration (VHA) Office of Rural Health (ORH) in 2006 (38 USC § 7308) to conduct, coordinate, promote and disseminate research on issues that affect the nearly five million Veterans who reside in rural communities. The mandate also requires ORH to develop, refine and promulgate policies, best practices, lessons learned, and innovative and successful programs.

ORH fulfils its mission by supporting targeted research, developing innovative programs and identifying new care models. Working through its five Veterans Rural Health Resource Centers as well as partners from academia, state and local governments, private industry and non-profit organizations, ORH strives to break down the barriers separating rural Veterans from quality care.

NOMAD uses the Salesforce Development Platform (SFDP) VA and is hosted in a Federal Risk Authorization Management Program (FedRAMP) certified cloud. The high-level architecture includes a database with an easy to configure graphical user interface (GUI) to input and recall information, workflows, reports and dashboards. The Salesforce architecture allows developers to combine and automate processes that may have been disconnected in the past. It also allows the team to create a single point of entry for all ORH data.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*

- *Whether 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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *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?*

Salesforce Government Cloud was granted a full ATO by Deputy CIO Service Delivery and Engineering (SD&E), for all applications that reside on the platform. The IT System name is Salesforce Development Platform (SFDP) VA; it is owned by the Office of Information Technology (OI&T), Enterprise Program Management Office (ePMO). The purpose of the IT system is to allow business lines and IT to deliver faster more secure solutions by building on a commercially available Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) product called Salesforce. Salesforce allows the configuration of a graphical user interface (GUI) to provide data entry, workflows, automation, and reporting and dashboards.

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

The ORH-NOMAD application is a streamlined solution to manage the lifecycle of ORH-funded initiatives aimed at increasing access to care for the 2.8 million rural Veteran population.

NOMAD Goals:

- Provide a single location for tracking all ORH activity
- Support and approve funding requests for current and future years
- Provide real-time data reporting for responding to congressional inquiries
- Create an environment that is accessible and suitable for use by VHA staff ranging from local Clinicians to VISN leadership

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.

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 Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integration Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Unique Identifying Information (list below)

Additional SPI: Operational Cost Comments, Project Budget Comments, Project Updates, Program Evaluation, Program Management Responses6.1

PII Mapping of Components

Active Directory Federated Services (ADFS) consists of **3** key components: IAM, ADFS, and Access VA. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **NOMAD** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	**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**
The Salesforce Development Platform (SFDP) use two VA Identity and Access Management services to validate user login information. The validation of VA employees is done through ADFS and end user information is validated using Access VA and their internal resources.	Yes	Yes	First Name, Last Name	Information is used project and FTE tracking	All VA employees use their PIV to sign into SFDP using ADFS. This IAM VA service checks the presented A credentials from their PIV card against VA's Active Directory. If an employee is not a user in Active Directory, then they will not have access to SFDP.

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Records (or information within records) in NOMAD include annual program and project details, budgetary information, project measures, and program and project narratives. All data in NOMAD is created in NOMAD or requested within the application except for the Account hierarchy. NOMAD uses the shared Account hierarchy to associate medical facilities with projects. Generally, information is entered directly by the end user or and ORH user that has partnered with the end user to ensure the data is entered into NOMAD. Additionally, the application takes the data entered by users and the project-level and aggregates it to the program for holistic visibility.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information and data in NOMAD is collected directly from the users during windows managed by ORH. Programs are created and maintained by ORH. Projects are entered by end users during the RFA window (or in partnership with ORH). Program Budget Change Requests (P-BCRs) are created by ORH users and end users after the RFA window is closed and the budgets are locked. Measures are entered by ORH users and end users throughout the year on a quarterly basis. All data is entered directly by either ORH users or VA users from medical centers.

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

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.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

ORH ensures data accuracy and integrity through several processes:

- Multi-step approval workflows to ensure all funded activity is validated a local, regional, and national leadership
- Users are only able to access data in accordance with their user role
- Data modifications are limited to specific fields and tracked through field history
- ORH takes weekly backups of key data fields
- ORH validates budget and Veteran impact data against external systems

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

There are no ORH-specific controls in place.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

Principle of Purpose Specification: 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:
NOMAD collects First Name and Last Name, which may be considered Personally Identifiable Information (PII). Due to the sensitive nature of this data, there is a risk that if the data were accessed by an unauthorized individual or otherwise breached, it could be exposed.

Mitigation:
Depending on level of authority granted to the user by ORH, each user will have a specific level of access to based on permission sets. The permissions will be reviewed on a regular basis to ensure that appropriate information is shared with appropriate users. NOMAD also employs the standard VA required security measures designed to ensure that the information is not inappropriately disclosed or released.

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 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.

- **First Name:** Used to capture the first name of a personnel line item for a program or project.
- **Last Name:** Used to capture the last name of a personnel line item for a program or project.
- **Operational Cost Comments:** Open text field used to capture additional comments about the purpose of an operational cost for a program.
- **Project Budget Comments:** Open field used sed to capture additional comments about the purpose of an budget line for a project.
- **Project Updates:** Open text field used sed to capture quarterly project updates.
- **Program Evaluation:** Open text field used sed to capture quarterly program progress.
- **Program Management Responses:** Open text field used sed to capture quarterly program management updates and needs.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Salesforce is used to run reports. The system does not create or make available new or previously unutilized information about an individual.

2.3 How is the information in the system secured?

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

This is not applicable to NOMAD.

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

This is not applicable to NOMAD.

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

No additional specific measures have been taken to meet the requirements of OMB Memorandum M-06-15. NOMAD complies will all standard VA requirements.

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>

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.

User accounts for NOMAD are created with specific user privileges based on the user's role. Prior to accessing NOMAD, users registration request are reviewed by a designated ORH approver by looking at the Contact, facility, and requested level of access. User records are controlled through credentials that are managed by the application. Access to information in the system is restricted to authorized personnel on a need-to-know basis by means of passwords protections, authorized user identification codes and/or PIV card login authentication. Additionally, access to records is managed by the role and sharing in place in NOMAD. Users are granted access to programs and projects based on their necessary level of access.

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

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

- First Name
- Last Name
- Operational Cost Comments
- Project Budget Comments
- Project Updates
- Program Evaluation
- Program Management Responses

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

The information is retained following the policies and schedules of VA's Records Management Service and NARA in "Department of Veterans Affairs Records Control Schedule 10-1". Record Control Schedule 10-1 can be found here: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

SFDP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFDP records are retained according to Record Control Schedule 10-1 Section 4. Record Control Schedule 10-1 can be found here: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

3.4 What are the procedures for the elimination of SPI?

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

Active Data stays on disk until the VA deletes it. All data will be retained within SFDP until it is required to be deleted according to the Record Control Schedule 10-1. Log data is retained by Salesforce for a year.

When hard drives and backup tapes are at their end of life, the media is sanitized based on Salesforce's Media Disposal Policy. Hard drives are overwritten using a multiple---pass write of complementary and random values. If it wipes successfully, we will return the disk or array to the vendor. If it fails during the wiping process we retain and destroy (i.e., degauss, shred, or incinerate). Backup tapes are degaussed prior to disposal. Specifics on the sanitization process are below.

Salesforce has an established process to sanitize production backup disks and hard drives prior to disposal, release out of salesforce's control, or release to the vendor for reuse. Production backup disks and hard drives are sanitized or destroyed in accordance with salesforce's Media Handling Process. All data is handled and located in VA own Salesforce's servers in Herndon, VA and Chicago, IL in the Salesforce Government Cloud server classification. Said information is handled with proper authority and scrutiny. Hard drives are sanitized within the data center facility using a software utility to perform a seven---pass overwrite of complementary and random values. If the drives wipe successfully, the hardware will be returned to the lessor. If the drive fails during the wiping process the drives are retained within a locked container within the salesforce data center facilities until onsite media destruction takes place. Leasing equipment provides salesforce with the opportunity to use the latest equipment available from vendors.

Periodically, a third-party destruction vendor is brought on---site to perform physical destruction of any hard drives that failed overwrite. A certificate of destruction is issued once the media is physically destroyed. Electronic data and files of any type, including PII, Sensitive Personal Information (SPI), and more are destroyed in accordance with the Department of Veterans' Affairs VA Directive 6500 (January 24, 2019):
https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf

When required, this data is deleted from their file location and then permanently deleted from the deleted items o0072 Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. The OIT Chief/CIO will be responsible for identifying and training OIT staff on VA media sanitization policy and procedures. The ISO will coordinate and audit this process and document the audit on an annual basis to ensure compliance with national media sanitization policy.

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

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

Information is not repurposed for any other reasons.

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.

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.

Privacy Risk:
The risk to maintaining data within the SFDP is that longer retention times increase the risk that information can be compromised or breached.

Mitigation:
To mitigate the risk posed by information retention, the SFDP adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the team will

carefully dispose of the data by the determined method as described in question 3.4. All electronic storage media used to store, process, or access VA records will be disposed of in adherence with the latest version of VA Handbook 6500.1, Electronic Media Sanitization.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Identity and Access Management (IAM) - Active Directory Federated Service (ADFS)	IAM ADFS Provisioning Service provides self- service options for internal VA users for centralized creation,	The ADFS servers pass a token to the SFDP that validates a VA internal user, via their federated ID, as a current credentialed user of VA systems.	Access credentials via login credentials along with integrating the PIV card and eToken security fobs.

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*
	modification, deletion and suspension for user accounts based on business processes and interactions defined by applications or systems.		

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

<u>Privacy Risk:</u>
There is a risk that information may be shared with unauthorized VA personnel.

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

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

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.

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

Privacy Risk:

There is no data being shared outside of the Department. If there is data being shared outside of the department in the future, access controls will be implemented based on MOUs, contracts or agreements.

Mitigation:
VA has contracted Salesforce Inc. to deliver services that include maintaining VA data. A contract is in place that clearly articulates Salesforce's roles and responsibilities. Authorized Salesforce personnel access user level data to provision and provide the Salesforce service. Access is controlled by authentication and is restricted to authorized individuals. Salesforce's security policies address the required security controls that must be followed in order to protect PII.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

The ORH-NOMAD application does not contain any PHI, SPI or exclusive information and as such a privacy notice is not provided to users. Additionally, all data entered into the application is voluntary and used for the sole purpose of requesting and tracking ORH funded activities.

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

This question does not apply as ORH-NOMAD does not contain PHI or SPI data.

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

This question does not apply as ORH-NOMAD does not contain PHI or SPI data.

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.

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:
This does not apply as ORH-NOMAD does not contain PHI or SPI data.

Mitigation:
This does not apply as ORH-NOMAD does not contain PHI or SPI data.

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?

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

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).

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.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Requestors may submit a FOIA request. Submitting a written FOIA request signed by the requestor(s) and reasonably describing the records sought to the VHA Central Office FOIA Service at 810 Vermont Avenue, NW (10A7) Washington, DC 20420, by fax at 202-273-9381, or via email at vhafoia2@va.gov. The VHA FOIA Office will obtain the requested records from the VHA Compliance and Business Integrity Office and respond to the request as appropriate.

Per the Privacy Act, only the subject of the record (First Party Access) or appropriate designee (Third Party Access) can request information. In addition, Information collected may be shared with VHA employees, contractors, and other service providers as necessary to respond to a request, provide a service, administer clinical treatment, solicit payment or as otherwise authorized by law. Information will not be shared with, or accessible by, any other entity without prior approval from CBI and review of data security and safety plans.

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

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

An individual who seeks access to or wishes to contest records maintained under his or her name in this system may write, call or visit the VHA Office of Compliance and Business Integrity (10E1A) Department of Veterans Affairs, 810 Vermont Avenue, NW. Washington, DC 20420.
202-745-8000 Ext. 55533.

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.

This question does not apply as ORH-NOMAD does not contain PHI or SPI data.

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

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

An individual who seeks access to or wishes to contest records in this system may write, call or visit the VHA Office of Compliance and Business Integrity (10B3) Department of Veterans Affairs, 810 Vermont Avenue, NW. Washington, DC 20420. 202-745-8000 Ext. 55533.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Privacy Risk:
There is a risk that individuals whose records contain incorrect information may not receive notification of appointments, prescription medications, and test results. Furthermore, incorrect information in a health record could result in improper diagnoses and treatments.

Mitigation:
SFDP mitigates the risk of incorrect information by authenticating information and validating data accuracy using the resources discussed in question 1.4. Privileged users will access online records

other than their own, consistent with their authority and organizational affiliations using PIV and based on permission-based access.

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?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

User roles identify role-specific access to the system and data. To receive access to NOMAD, an ORH Admin with appropriate permissions must approve their request. The approver will the requested access level, the user's role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level contract of the information and data. This information is documented in the user provisioning process with the Digital Transformation Center (DTC).

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The contractors who provide support to the system are required to complete annual VA Privacy and information Security and Rules of Behavior training via the VA's Talent Management System (TMS). The Office of Contract Review operates under a reimbursable agreement with VA's Office of

Acquisition, Logistics and Construction (OALC) to provide pre-award, post-award, and other requested reviews of vendors' proposals and contracts.

System Owner and Contracting Officer Representative (COR) is the individual to accept and amend any incoming or outgoing contracts involving Salesforce Development Platform VA.

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

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

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

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

1. The Security Plan Status: Approved
2. The Security Plan Status Date: 24-Feb-2021
3. The Authorization Status: Authorization to Operate (ATO)
4. The Authorization Date: 18-Mar-2021
5. The Authorization Termination Date: 17-Dec-2023
6. The Risk Review Completion Date: 12-Mar-2021
7. The FIPS 199 classification of the system: Moderate

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).

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.

The ORH-NOMAD VECMS Salesforce application utilizes the VAEC.

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Response not required due to 9.1.

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.

This is not applicable to NOMAD.

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.

Response not required due to 9.1.

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 is not applicable to NOMAD.

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**

ID	**Privacy Controls**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

JULIE C. DRAKE 969177

Digitally signed by JULIE C. DRAKE 969177
Date: 2022.09.09 07:39:45 -06'00'

Privacy Officer, Julie Drake

JAMES BORING

Digitally signed by JAMES BORING
Date: 2022.09.09 08:45:46 -04'00'

Information Systems Security Officer, James Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2022.09.09 07:26:17 -04'00'

Information System Owner, Michael Domanski

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).