Privacy Impact Assessment for the VA IT System called:

Veterans Integrated Registries Platform (VIRP) Assessing

Veterans Health Administration (VHA)

Health Registry (HREG)

eMASS ID #187

Date PIA submitted for review:

06/05/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Louis McCrutchen	Louis.Mccrutchen@va.gov	202-461-8872
Information System Owner	Tony Sines	Tony.Sines@va.gov	202-270-1432

Abstract

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

The Veterans Integrated Registries Platform (VIRP) is a centralized architectural platform for the national health registries and is comprised of standardized common patient data and registry-specific data elements. VIRP provides clinician on-demand reporting capabilities and integrate ad-hoc reporting/query capabilities. VIRP provides a web portal to enable one entry point for all registries and VIRP provides a back-end data base with a subset for each registry that includes common data and then registry specific 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:

1 General Description

A. *What is the IT system name and the name of the program office that owns the IT system?*

Veterans Integrated Registries Platform (VIRP) Assessing, Veterans Health Administration (VHA) Health Registry (HREG)

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

The Veterans Integrated Registries Platform (VIRP) is a centralized architectural platform for the national health registries and is comprised of standardized common patient data and registry-specific data elements. VIRP provides clinician on-demand reporting capabilities and integrate ad-hoc reporting/query capabilities. VIRP provides a web portal to enable one entry point for all registries and VIRP provides a back-end data base with a subset for each registry that includes common data and then registry specific data.

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

VA owned and VA operated.

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?*

There are over a million patients' information between the registries that make up VIRP. The typical client or affected individual is a Veteran or active service member.

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

Description, purpose of collecting information is for reporting on various patient cohorts.

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

VIRP consists of 11 registries and are listed in the Internal connections table below.

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?*

VIRP is operated at AITC and no other site.

3. Legal Authority and SORN

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

SORN 121VA10 – National Patient Databases, VA (Formerly 121VA19) states the authority to maintain the system is Title 38, United States Code, Section 501. The SORN can be found at the following website 2023-07638.pdf (govinfo.gov)

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The SORN will not require amendment or revision. The system does not use cloud technology.

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 processes.

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

The completion of this PIA will not result in technology changes.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on *these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.*

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements:

- Theatre of War Indicator - Operation Enduring Freedom (OEF)/ Operation Iraqi Freedom (OIF) Indicator(s)
- Date of Death
- Last Service Separation Date
- Patient Electronic Data Interchange Personal Identifier (EDIPI)
- Laboratory Results
- Marital Status
- Branch of Service
- Unit Component
- Loss/Separation Date Eligible Deployment Segments
- Start Date Eligible Deployment Segments
- End Date Eligible Deployment Segments

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

- Location Eligible Deployment Segments
- Occupation Type During Eligible Deployment Segments
- Health Information such as: Allergies, Immunizations, Inpatient/Outpatient data, Lab data, etc.

PII Mapping of Components (Servers/Database

VIRP consists of 12 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **VIRP** 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**
Multiple Sclerosis Surveillance Registry (MSSR)	Yes	Yes	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email address Current Medications, Previous Medical Records, Race/Ethnicity, OEF/OIF service indicator, date of death, last Service Separation date, patient EDIPI. Lab	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles

			results, Marital status		
Traumatic Brain Injury (TBI) Registry	Yes	Yes	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email address Current Medications, Previous Medical Records, Race/Ethnicity, OEF/OIF service indicator, date of death, last Service Separation date, patient EDIPI. Lab results, Marital status	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles
Airborne Hazards and Open Burn Pit Registry (AHOBPR)	Yes	Yes	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email address Current Medications, Previous Medical Records, Race/Ethnicity, OEF/OIF service indicator, date of death, last Service	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles

			Separation date, patient EDIPI. Lab results, Marital status		
Kidney Dialysis Registry (KDR)	Yes	Yes	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email address Current Medications, Previous Medical Records, Race/Ethnicity, OEF/OIF service indicator, date of death, last Service Separation date, patient EDIPI. Lab results, Marital status	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles
Hearing Registry (HR)	Yes	Yes	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email address Current Medications, Previous Medical Records, Race/Ethnicity, OEF/OIF service	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles

			indicator, date of death, last Service Separation date, patient EDIPI. Lab results, Marital status		
Amputee Registry (AR)	Yes	Yes	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email address Current Medications, Previous Medical Records, Race/Ethnicity, OEF/OIF service indicator, date of death, last Service Separation date, patient EDIPI. Lab results, Marital status	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles
Breast Care Registry (BCR)	Yes	Yes	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email address Current Medications, Previous Medical Records,	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles

			Race/Ethnicity, OEF/OIF service indicator, date of death, last Service Separation date, patient EDIPI. Lab results, Marital status		
Embedded Fragment Registry (EFR)	Yes	Yes	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email address Current Medications, Previous Medical Records, Race/Ethnicity, OEF/OIF service indicator, date of death, last Service Separation date, patient EDIPI. Lab results, Marital status	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles
Eye Injury Data Store (EIDS)	Yes	Yes	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email address Current Medications,	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles

			Previous Medical Records, Race/Ethnicity, OEF/OIF service indicator, date of death, last Service Separation date, patient EDIPI. Lab results, Marital status		
Ionizing Radiation Registry (IRR)	**yes**	**yes**	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email address Current Medications, Previous Medical Records, Race/Ethnicity, OEF/OIF service indicator, date of death, last Service Separation date, patient EDIPI. Lab results, Marital status	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles
Agent Orange Registry (AOR)	**yes**	**yes**	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles

			address Current Medications, Previous Medical Records, Race/Ethnicity, OEF/OIF service indicator, date of death, last Service Separation date, patient EDIPI. Lab results, Marital status		
Gulf War Registry (GWR)	**yes**	**yes**	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number, email address Current Medications, Previous Medical Records, Race/Ethnicity, OEF/OIF service indicator, date of death, last Service Separation date, patient EDIPI. Lab results, Marital status	Patient identification and verification	Centralized access control with two factor authentications and registry-specific roles

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?

Information is collected from the individual as part of Registrant Portal, and from other sources – all of the registry internal components listed in the table above.

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.

Corporate Data Warehouse (CDW) is the primary source of aggregated data. It would not be beneficial for VIRP to collect information that already exists.

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

TBI and Amputee registries create reports based on scores calculated from survey answer options. MSSR tracks MS related data and uses it for aggregated reporting on Veterans with MS.

1.3 How is the information collected?

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

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

Information will be collected for VIRP from the various sources including VistA and CDW into the Registry Staging databases. The Registries will then be loaded into the production environment. Data will also be transferred by web services from the Master Person Index (MPI) and from DOD via secure exchange of files.

The data from Veterans is directly inputted into the TBI, Amputee, and MSSR components through the VIRP user interface.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

Information is not collected on a form and is not subject to the Paperwork Reduction Act.

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 sources of data that VIRP will use are all VA-Approved data sources. These sources are systems of record, and their data has already been vetted for accuracy.

There is an assumption of accuracy since the information is collected directly from the subject or fed into the system from existing systems. The source data is checked for accuracy at the point of patient care. All revisions/corrections to the source data are immediately available in VIRP.

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?

VIRP uses VA Master Person Index (MPI) to validate whether the individual is a real person and that the data elements are accurate. Without validation the individual cannot be added to the registry. (AOR, GWR, and IRR only at this time)

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C 501.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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.

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

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

<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.

Follow the format below when entering your risk assessment:

<u>Privacy Risk:</u> VIRP will collect Personally Identifiable Information (PII) and Protected Health Information (PHI) for use in the registries identified in Internal Components Table above.
Due to the highly sensitive nature of this data, there will be a risk that, if the data were accessed by an unauthorized individual or otherwise breached, and serious personal, professional or financial harm may result for the individuals affected.

<u>Mitigation:</u> The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is able to better protect the individual's information.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Name	Patient/Record Identification	Not used
Social Security Number	Patient Identification	Not used
Date of Birth	Patient/Record Identification	Not used
Mailing Address	VAMC Identification	Not used
Zip Code	VAMC Identification	Not used
Phone Number	Patient Contact Information	Not used
Email Address	Patient Contact Information	Not used
Current Medications	Research and Analysis	Not used
Previous Medical Records	Research and Analysis	Not used
Race/Ethnicity	Research and Analysis	Not used
Theater of War OEF/OIF	Research and Analysis	Not used
Date of Death	Research and Analysis	Not used
Last Service Separation Date	Research and Analysis	Not used
Patient EDIPI	Patient/Record Identification	Not used
Laboratory Results	Research and Analysis	Not used
Marital Status	Research and Analysis	Not used
Gender	Research and Analysis	Not used

Branch of Service	Research, Analysis & Eligibility	Not used
Unit Component	Research, Analysis & Eligibility	Not used
Loss/Separation Date Eligible Deployment Segment	Research, Analysis & Eligibility	Not used
Start Date Eligible Deployment Segment	Research, Analysis & Eligibility	Not used
End Date Eligible Deployment Segment	Research, Analysis & Eligibility	Not used
Location Eligible During Deployment Segment	Research, Analysis & Eligibility	Not used
Occupation Type During Eligible Deployment Segment	Research, Analysis & Eligibility	Not used
Health Information	Research, Analysis & Eligibility	Not used

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

Patient-Registry inclusion indicators allow owners to access common demographics and clinical data, along with unique registry specific information. The new data that is added becomes part of the registry. The data can be imported by various end users i.e. providers that are gathering information from the veterans based on the questionnaire type. Clinical and demographics data is specific to the patient and independent of their inclusion in any registry. The application layer for each registry is independent of all registry functions but is unique to that registry. The filter functions for the data “extraction and update” interface are independent of the registry itself (and are unique to each data source).

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.

VIRP does not create or make available new or previously unutilized information about individuals.

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?

VIRP employs TLS 1.2 for protection of data in transit, and data at rest resides on AITC secure servers.

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

VIRP has reduced the need for SSN storage and transmission. SSNs are only displayed as the last 4.

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

The Office of Management and Budget (OMB) Memorandum M-06-15 is inherited by the VA Rules of Behavior (ROB) per VA Handbook 6500. VA Rules of Behavior are part of a comprehensive program to convey information security requirements and expected behavior of all individuals with access to VA information and information systems. VIRP adheres to the directives outlined in OMB Memorandum M-06-15 and M-06-16 concerning PII/PHI.

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

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

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

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

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

2.4a How is access to the PII determined?

The System of Record Notice(s) (SORNs) that apply to VIRP define the information collected from Veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a Veteran’s eligibility and benefits, such as eligibility, compensation, or education.

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

The criteria, procedures, controls, and responsibilities regarding access to VIRP are documented in the VIRP Access Control policy. Additionally, VACCRs 17 security related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and information processed, stored and transmitted are documented within the Governance, Risk and Compliance (GRC) tool.

2.4c Does access require manager approval?

Yes, VIRP requires manager approval through the use of VA tools for access creation.

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

Access control logs at the VA level are monitored in accordance with VA policies and procedures.

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

All VA personnel are responsible for assuring safeguards for PII. The Facility Telehealth Coordinator (FTC) assures safeguards for the PII at the VA level and is touched on in specific HIPAA and other VA trainings.

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*

- Name
- Social Security Number
- Date of Birth
- Mailing Address
- Zip Code
- Phone Number
- Email Address
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Theatre of War OEF/OIF service indicator
- Date of Death
- Last Service Separation Date
- Patient EDIPI
- Laboratory results
- Marital Status
- Gender
- Branch of Service
- Unit Component
- Loss/Separation Date Eligible Deployment Segments

- Start Date Eligible Deployment Segments
- End Date Eligible Deployment Segments
- Location Eligible Deployment Segments
- Occupation Type During Eligible Deployment Segment
- Health Information such as: Allergies, Immunizations, Inpatient/Outpatient data, Lab data, etc

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.*

Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule, 5.2, item 020..

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

Yes.

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

Per the SORN 121VA10A7, “Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule, 5.2, item 020. The records are disposed of when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes.

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.*

VIRP data that is authorized for destruction is eliminated through utilization of the following methods:

- Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization.
- Disposition of Printed Data:
    - Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

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.

In compliance with the Health Registries (HREG) and VA standard procedures the developments cannot use any PII for testing in the development environment and any screen shots shared in end user training material or user guides. The selected development team members and clinicians participating in User Accepting Testing (UAT) are granted elevated privileges for the Software Quality Assurance (SQA) and PreProduction environments perform testing and participate in troubleshooting of identified defects. The SQA and PreProduction environments are housed on AITC servers and protected by a firewall.

Additionally, VIRP is designed to comply with the 2-Factor-Authentication (2FA) and HREG system administrators grant access to VIRP/registry users on a case-by-case basis assigning user roles with a defined set of permissions for each registry and the overall VIRP platform. Unauthorized users can view a description of the health registries but cannot access data and content collected within the registry. Researchers as well as clinicians and clinical staff are granted access to the registries only upon approval by the business owner.

<u>3.6 PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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: There is a risk that the information maintained by VIRP could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, once VIRP records are cleared for destruction, VIRP will endeavor to adhere to the NARA General Records Schedule. When the retention date is reached for a record, the individual's information is carefully disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule, 5.2, item 020. In the interim period of system development access to system data will be restricted to only personnel with a clear business requirement. The data will be encrypted to Federal Information Processing Standard (FIPS) 140-2 standards or its successor.

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***
Corporate Data Warehouse (CDW)	To access electronic health record data based on registry cohort criteria	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number • Email Address • Current Medications • Previous Medical Records • Race/Ethnicity • Theatre of War • Date of Death • Last Service Separation Date • Patient EDIPI • Laboratory results • Marital status • Gender	Structured Query Language (SQL) Server Integration Services (SSIS). Web services to manage and execute the Extract, Transform, and Load (ETL) packages.
VA Master Person Index (MPI)	To validate patient identifying data and mappings between	• Patient EDIPI • ICN	Web Service: Simple Object Access

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***
	patient identifiers, such as electronic data interchange personal identifier (EDIPI) and Integration Control Number (ICN).		Protocol (SOAP) XML
Veterans Health Information Systems Technology Architecture (VistA)	Utilized for analysis and research to enhance patient population care	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number • Email Address • Current Medications • Previous Medical Records • Race/Ethnicity • Theatre of War • Date of Death • Last Service Separation Date • Patient EDIPI • Laboratory results • Marital Status • Gender	Secure electronic transfer via Hypertext Transfer Protocol Secure (HTTPS)/ Health Level7 (HL-7)
Veteran Identity/Eligibility Reporting System (VIERS)/ VA/DoD Identity Repository (VADIR)	VIERS provides Person demographic, contact, military service and other benefits information including benefits eligibility profile. VADIR provides deployment information	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number • Email Address • Current Medications • Previous Medical Records • Race/Ethnicity • OEF/OIF service indicator	Structured Query Language (SQL) Server Integration Services (SSIS).

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***
		• Date of Death • Last Service Separation Date • Patient EDIPI • Laboratory results • Marital Status	
Data Access Services (DAS)	DAS sends registry records to DoD	• Name • Social Security Number • Date of Birth • Gender • Military Branch Name • Patient AHOBPR Questionnaire	PDF, Web service: RESTful
Enterprise Veterans Self Service (EVSS)	Provides gateway for veterans and service members to access the AHOBPR web application	Patient EDIPI	Secure electronic transfer via Hypertext Transfer Protocol Secure (HTTPS)
VA Profile	VA Profile provides Veterans' identity, contact information, military service, enrollment, eligibility for VA services and benefits, socio-economic, demographic, customer experience, interaction history and shared data from health, benefits and cemetery administrations are automatically synchronized across all VA systems.	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number • Email Address • Current Medications • Previous Medical Records • Race/Ethnicity • Theatre of War • Date of Death • Last Service Separation Date • Patient EDIPI • Laboratory results	Secure electronic transfer via Hypertext Transfer Protocol Secure (HTTPS)

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***
		• Marital Status • Gender	

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> The privacy risk associated with maintaining PII/PHI will be that sharing data within the Department of Veteran's Affairs could happen and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

<u>Mitigation:</u> The principle of need-to-know will be strictly adhered to by the personnel who will use VIRP. Only personnel with a clear business purpose will be allowed access to the system and the information contained within.

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***
DOD Embedded Fragment Registry (EFR) and DOD Public Health Command	This will be the business flow for data between VA & DOD	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Phone Number • Email Address • Current Medications • Previous Medical Records • Race/Ethnicity • Theatre of War • Date of Death • Last Service Separation Date • Patient EDIPI • Laboratory results • Marital Status	MOU between Defense Manpower Data Center (DMDC) and VA; Agreement # M1315	Secure electronic transfer via Hypertext Transfer Protocol Secure (HTTPS), Web services to manage and execute the Extract, Transform, and Load (ETL) packages
DOD Joint Pathology Center	This will be the business flow for data between VA & DOD	• Name • Social Security Number • Date of Birth • Mailing Address • Zip Code	MOU between Defense Manpower	Secure electronic transfer via

		- Phone Number - Email Address - Current Medications - Previous Medical Records - Race/Ethnicity - Theatre of War - Date of Death - Last Service Separation Date - Patient EDIPI - Laboratory results - Marital Status	Data Center (DMDC) and VA; Agreement # M1315	Hypertext Transfer Protocol Secure (HTTPS), Web services to manage and execute the Extract, Transform, and Load (ETL) packages
DOD Embedded Fragment Analysis Laboratory	This will be the business flow for data between VA & DOD	- Name - Social Security Number - Date of Birth - Mailing Address - Zip Code - Phone Number - Email Address - Current Medications - Previous Medical Records - Race/Ethnicity - Theatre of War - Date of Death - Last Service Separation Date - Patient EDIPI - Laboratory results - Marital Status	MOU between Defense Manpower Data Center (DMDC) and VA; Agreement # M1315	Secure electronic transfer via Hypertext Transfer Protocol Secure (HTTPS), Web services to manage and execute the Extract, Transform, and Load (ETL) Packages
IAM/DoD		- Name - Social Security Number - Date of Birth - Mailing Address - Zip Code - Phone Number - Email Address - Current Medications - Previous Medical Records - Race/Ethnicity - Theatre of War - Date of Death - Last Service Separation Date - Patient EDIPI - Laboratory results - Marital Status	MOU between Defense Manpower Data Center (DMDC) and VA; Agreement # M1315	Secure electronic transfer via Hypertext Transfer Protocol Secure (HTTPS)

		• Gender		

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> The privacy risk associated with sharing VA sensitive data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused. Additionally, there is a privacy threat of a breech during the transmission of the data.

<u>Mitigation:</u> In order to share data with the Department of Defense (DoD), VIRP utilizes a Memorandum of Understanding (MOU) between the Defense Manpower Data Center (DMDC) and the Department of Veterans Affairs (Agreement #M1315) which outlines security/access controls for storing data, use of transferred data and governs data transfer safekeeping.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the

Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in several ways:

The System of record Notice (SORN) – National Patient Databases, 121VA10 The SORN can be found online at 2023-07638.pdf (govinfo.gov)

This Privacy Impact Assessment (PIA) also serves as notice of the Veterans Integrated Registries Platform (VIRP) system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

Individuals are provided notice when entering their information into the data base and the Notice of Privacy Practices is provided to all Veterans.

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

Notice was provided.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter. This Privacy Impact Assessment (PIA) also serves as notice as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means. A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority, and the conditions under which the information can be disclosed. Notice is provided in the SORN: If notice was provided in the Federal Register, provide the citation. SORN Full List of VA Privacy Act Systems of Records"

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.

Veterans add information to the registry which is strictly voluntary. For the information that is fed into the system from existing data bases, Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

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

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

> **Privacy Risk:** There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.
>
> **Mitigation:** This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NOPP is also available at all VHA medical centers from the facility Privacy Officer.
> The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

SORN 121VA10 states under notification procedures that individuals who wish to determine whether this system of records contains information about them should contact the Director of National Data Systems (10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772. Inquiries should include the person's full name, Social Security number, location and dates of employment or location and dates of treatment, and their return address.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

In accordance with SORN 121VA10, RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above or write or visit the VA facility location where they normally receive their care. A request for access to records must contain the requester’s full name, address and telephone number, be signed by the requester and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

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)?

VIRP is not exempt from the access provisions of the Privacy Act.

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

VIRP is a Privacy Act system.

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

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

In accordance with SORN 121VA10 CONTESTING RECORD PROCEDURES: Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

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.

VHA has a documented process for individuals to request inaccurate PII be corrected or amended and a process for review to determine if correction or amendment is appropriate. The policy complies with both the Privacy Act, VA regulations and the HIPAA Privacy Rule. Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every VHA Privacy Act SORN contact information on Contesting Record Procedure which informs the individual who to contact for redress. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

VHA has a documented process for individuals to requested inaccurate PII be corrected or amended and a process for review to determine if correction or amendment is appropriate. The policy complies with both the Privacy Act, VA regulations and the HIPAA Privacy Rule. Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every VHA Privacy Act SORN contact information on Contesting Record Procedure which informs the individual who to contact for redress. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: the risk of incorrect information in an individual's records is mitigated by authenticating information when possible, Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses the process for requesting an amendment to one's records.

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?

Veterans Integrated Registries Platform (VIRP) stakeholders are responsible to evaluate and grant access (roles) accordingly to their respective registries, and those users are employed by the VA and will have had to complete the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training.

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?

VHA Support Service Center (VSSC) users have access to VIRP for pulling Traumatic Brain Injury (TBI) data. VIRP stakeholders and stakeholders from other agencies are responsible to establish the criteria for what PII within the registry can be shared.

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.

Continuity of the security requirements below will be met by the VIRP framework, which will contain the layers of access, as follows:

- Enterprise Access: To be granted to users requiring reports and information on an enterprise level. Enterprise access will also include access to Veterans Integrated Service Network (VISN) level and local level functionalities.
- VISN Access: To be granted to users requiring reports and information on a VISN specific level. The access is restricted to reports and information from that user's assigned VISN. VISN level access will also include local level functionality for sites within the VISN.
- Local Level: To be granted to users requiring reports and information on a local level. Users with local access will be restricted to reports and information for their assigned location. Local users will not have access to VISN or Enterprise reports or information. Local level will be the most restrictive level of access.
- Registry Read: To be granted to users for reporting needs.
- Registry Update: To be granted to users for inputting/updating records within a registry.
- Registry Administer: To be granted to users for administration of users and advanced functions for a given registry.

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.

No. If required, contractors who provide support to the system are required to complete annual VA Privacy and Information Security, HIPAA and Rules of Behavior training via the VA's Talent Management System (TMS). Review of access to all systems is done on a quarterly basis by the ISO and the security engineer. Clearance is required for each person accessing the system. Contracts are reviewed annually by the Contracting Officer Representative (COR).

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual HIPAA, Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Signed
2. *The System Security Plan Status Date:* 12/14/2023
3. *The Authorization Status:* Authorized (ATO)
4. *The Authorization Date:* 07/11/2022
5. *The Authorization Termination Date:* 07/10/2025
6. *The Risk Review Completion Date:* 04/29/2022
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.***

VIRP has completed the A&A.

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)*

VIRP does not use cloud technology.

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.*

VIRP does not use cloud technology.

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.

VIRP does not use cloud technology.

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.

VIRP does not use cloud technology.

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).

VIRP does not use 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.

NANCY KATZ-JOHNSON Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.06.14 16:28:04 -04'00'

Privacy Officer, Nancy Katz-Johnson

LOUIS MCCRUTCHEN Digitally signed by LOUIS MCCRUTCHEN
Date: 2024.06.18 09:00:42 -04'00'

Information System Security Officer, Louis McCrutchen

TONY SINES Digitally signed by TONY SINES
Date: 2024.06.18 16:13:18 -05'00'

Information System Owner, Tony Sines

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).

A copy of the VHA Notice of Privacy Practices is found here https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090

121VA10 National Patient Database – VA 2023-07638.pdf (govinfo.gov)

Current SORN List (va.gov) https://www.oprm.va.gov/docs/Current_SORN_List_1_7_2022.pdf

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

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

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