Privacy Impact Assessment for the VA IT System called:

Veterans Integrated Registries Platform (VIRP)

Veterans Health Administration (VHA)

Date PIA submitted for review:

02/08/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202-870-1284
Information System Security Officer (ISSO)	Pedro Epting	Pedro.Epting@va.gov	703-483-5096
Information System Owner	Christopher Brown	Christopher.Brown1@va.gov	202-270-1432

Abstract

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

The Veterans Integrated Registries Platform (VIRP) will be a centralized Registry database platform and architectural framework for national health Registries that effectively manages Registries' data at a national level to support VHA in being a Veteran-centered, integrated organization providing excellence in health care, research, and education. Comprised of shared, standardized common patient data and Registry-specific data elements, VIRP will act as the backend database system architecture for seven (7) national health Registries, providing a cohesive database structure for the national Registry's front-end online Registry transaction processing and reporting functionalities. Four (4) additional new registries are currently in development and will be deployed on VIRP. VIRP will provide enhanced inter-operability and ease of use over its predecessor, Converged Registries Solution (CRS).

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.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *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?*
- *Does the system use cloud technology? 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.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*

- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

The Veterans Integrated Registries Platform (VIRP) is a single conceptual structure composed of multiple logical case-specific registries; this allows individuals to maintain registry information as applicable, while allowing more accurate research into the topics of each registry. VIRP will be active concurrent with the system it will replace Converged Registries Solution (CRS) until all existing health registries on CRS have been migrated.

The VRIP is a centralized, relational database framework and architectural platform for the registries in the Health Registries (HREG) program. This relational database assists in effectively managing national registry data to support the goal of the Veterans Health Administration (VHA) to be a Veteran-centered, integrated organization that provides excellence in health care, research, and education. Comprised of standardized common patient data and registry-specific data elements, VIRP provides the backend database architecture for each national health registry.

As VA moves forward with its registry solutions, it has identified opportunities for technological improvement. VA is shifting from individual registry solutions to a more holistic technical and functional integration of data that allows Veteran information to be collected more efficiently. In this way, registry users can make more efficient use of the registry data and analytical products to better manage individual Veterans and the general health of the cohort. Registry functions and products are available both in clinical and administrative contexts to facilitate action.

The current CRS design was analyzed through a review of CRS artifacts and interviews with subject matter experts. Based on this analysis, the VIRP effort will implement enhancements and improvements to the current architecture by employing a single VIRP Web portal with Web services. It will consolidate all registries into one Web portal system that accesses business logic and data to create reusable and common functionality.

The VIRP will continue to facilitate the national registries and act in accordance with enterprise-wide, VA-mandated requirements, such as those related to Privacy and Security, and user access to PHI and PII.

The VIRP will reside in Enterprise Operations (EO) Austin Information Technology Center (AITC) with an EO application code of CRE.

Planned interfaces for implementation in FY18: Corporate Data Warehouse (CDW), Master Person Index (MPI), Veterans Health Information Systems Technology Architecture (VistA), Veteran Identity/Eligibility Reporting System (VIERS)/ VA/DoD Identity Repository (VADIR), Data Access Services (DAS), Enterprise Veterans Self Service (EVSS) and VA Enterprise Messaging Infrastructure (eMI).

VIRP is accredited but migration from CRS has been delayed, the expected number of records should be approximately 4,593,192 within VIRP with increases every year.

Access to patient data within VIRP will be limited to those patients identified as belonging to a specific registry. Access controls are multi-layered and are specific to the assigned parameters and credentials of that individual user to allow "role-based" access.

Patient-Registry inclusion indicators allow owners to access common demographics and clinical data, along with unique registry specific information. Clinical and demographics data is specific to the patient and independent of their inclusion in any registry.

There will be seven (7) existing health registries supported by VIRP at the start of production. They are as follows: Breast Care Registry (BCR), Embedded Fragment Registry (EFR), VA Eye Injury Data Store (EIDS), Multiple Sclerosis Surveillance Registry (MSSR), Oncology Tumor Registry (ONC), Traumatic Brain Injury (TBI) Registry, and Airborne Hazards and Open Burn Pit Registry (AHOBPR).

The following four health registries will also be developed and deployed on VIRP: Kidney Disease Registry (KDR), Hearing Registry (HR), Amputee Registry (AR), and Transplant Registry (TR).

All information in this document regarding the information collected and maintained on the VIRP also applies to each of the health registries residing on the VIRP listed above.

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes. System of Record Notice (SORN) 121VA10P2– National Patient Databases, VA (Formerly 121VA19) states the authority to maintain the system is Title 38, United States Code, Section 501.

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.

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
Other Unique Identifying Number (list below)

In addition to the data collected above, VIRP will also collect the following: • Answers to the Airborne Hazards and Open Burn Pit Registry (AHOBPR) questionnaire completed by Veterans and Service members and clinical data relevant to each specific registry • 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 • 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 Segments • Health Information such as: Allergies, Immunizations, Inpatient/Outpatient data, Lab data, etc.

PII Mapping of Components

Veterans Integrated Registries Platform consists of 11 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Veterans Integrated Registries Platform and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) 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
Breast Care Registry (BCR)	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

			Previous Medical Records, Race/Ethnicity, OEF/OIF service indicator, date of death, last service, Separation date, patient EDIPI. Lab results, Marital status		authentications and registry-specific roles
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 authentication and registry-specific roles
VA Eye Injury Data Store (EIDS)	**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 authentication and registry-specific roles
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 results, Marital status	Patient identification and verification	Centralized access control with two factor authentication and registry-specific roles
Oncology Tumor Registry (ONC)	**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 authentication and registry-specific roles
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 authentication 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,	Patient identification and verification	Centralized access control with two factor authentication

			Race/Ethnicity, OEF/OIF service indicator, date of death, last service, Separation date, patient EDIPI. Lab results, Marital status		and registry-specific roles
Kidney Disease 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 authentication 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 indicator, date of death, last service, Separation date, patient EDIPI. Lab results, Marital status	Patient identification and verification	Centralized access control with two factor authentication and registry-specific roles
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 authentication and registry-specific roles
Transplant Registry (TR)	**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 authentication and registry-specific roles

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.

VIRP will be the centralized platform for the HREG registries. VIRP will therefore be a composite of information from the constituting registries. The registries will be as follows: Breast Care Registry (BCR), Embedded Fragment Registry (EFR), VA Eye Injury Data Store (EIDS), Multiple Sclerosis Surveillance Registry (MSSR), Oncology Tumor Registry (OncoTrax), Traumatic Brain Injury (TBI) Registry and Airborne Hazards and Open Burn Pit (AHOBPR). Future planned registries include: Kidney Disease Registry (KDR), Hearing Registry (HR), Amputee Registry (AR), and Transplant Registry (TR).

The VIRP system will extract data from VistA/CPRS, the Corporate Data Warehouse (CDW), the Theater Medical Data Store (TMDS) by means of a Department of Defense (DOD) interface, and from the Master Person Index (MPI). The means in which information collected and maintained on the VIRP also applies to each of the health registries residing on the VIRP listed above.

VIRP will also provide a means for clinicians to generate notes that are stored in CPRS.

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.

Information will be collected for VIRP via Structured Query Language (SQL) Server Integration Services (SSIS). Extract, Transform, and Load (ETL) packages load data from the various sources including VistA and CDW into Registry Staging databases. The Registries will be then loaded with data from the staging area to the preproduction and production environment. Data will also be transferred by web services from the Master Person Index (MPI) and from DOD via secure exchange of flat files.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose. This question is related to privacy control AP-2, Purpose Specification.

The data that will be pulled into VIRP will be utilized for analysis and research to enhance patient care, but not to provide individual patient care. In addition, the VIRP platform and its health registries (HREG) will provide a framework and tools for the health program offices to ensure that appropriate care is being provided to specific veteran patient populations. The registries hosted on the VIRP framework supports population health rather than direct patient care.

1.5 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.

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.

Patient-Registry inclusion indicators allow owners to access common demographics and clinical data, along with unique registry specific information. 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)

1.6 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

The Secretary of Veterans Affairs established guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

SORN 121VA10A7– 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 https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf

1.7 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: VIRP will collect Personally Identifiable Information (PII) and Protected Health Information (PHI) for use in the following registries: • Breast Care Registry (BCR) • Embedded Fragment Registry (EFR) • VA Eye Injury Data Store (EIDS) • Multiple Sclerosis Surveillance Registry (MSSR) • Oncology Tumor Registry (OncoTrax) • Traumatic Brain Injury (TBI) Registry • Airborne Hazards and Open Burn Pit (AHOBPR) • Kidney Disease Registry (KDR) • Hearing Registry (HR) • Amputee Registry (AR) • Transplant Registry (TR)

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.

Mitigation: 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 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.

The information contained in the list below is collected and maintained on the VIRP for use in the following health registries: Breast Care Registry (BCR), Embedded Fragment Registry (EFR), VA Eye Injury Data Store (EIDS), Multiple Sclerosis Surveillance Registry (MSSR), Oncology Tumor Registry (OncoTrax), Traumatic Brain Injury (TBI) Registry, Airborne Hazards and Open Burn Pit (AHOBPR), Kidney Disease Registry (KDR), Hearing Registry (HR), Amputee Registry (AR), and Transplant Registry (TR).

- Name - Used to identify veteran patient records.
- Social Security Number- Used to verify the identity of the veteran.
- Date of Birth - Used to identify veteran patient records
- Mailing Address – Used as demographic information, e.g. identify nearest VAMC
- Zip Code - Used as demographic information, e.g. identify nearest VAMC
- Phone Number – Used as patient contact information
- Email Address - Used as patient contact information

- Current Medications – Used for research and analysis
- Previous Medical Records – Used for research and analysis
- Race/Ethnicity – Used for research and analysis
- Theater of War OEF/OIF service indicator – Used for research and analysis
- Date of Death – Used for research and analysis
- Last Service Separation Date – Used for research and analysis
- Patient EDIPI - Used to identify veteran patient records
- Laboratory results – Used for research and analysis
- Marital Status – Used for research and analysis
- Gender – Used for research and analysis
- Branch of Service – Used for research and analysis and eligibility
- Unit Component – Used for research and analysis and eligibility
- Loss/Separation Date Eligible Deployment Segments – Used for research and analysis and eligibility
- Start Date Eligible Deployment Segments – Used for research and analysis and eligibility
- End Date Eligible Deployment Segments – Used for research and analysis and eligibility
- Location Eligible Deployment Segments – Used for research and analysis and eligibility
- Occupation Type During Eligible Deployment Segment – Used for research and analysis and eligibility
- Health Information such as: Allergies, Immunizations, Inpatient/Outpatient data, Lab data, etc. – Used for research and analysis and eligibility

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

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 and 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).

2.3 <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.

The System of Record Notice(s) (SORNs) that apply to this system 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.

The minimum-security requirements for VIRP's HIGH impact system will cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity.

AITC will employ all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

Users are trained how to handle sensitive information by taking VA Privacy and security awareness training and reading and attesting they understand the VA Rules of Behavior. Additionally, VIRP users must also take VA HIPPA focused training and VA Privacy and Information Security Awareness Training before gaining access to the VIRP system both are required to be taken on an annual basis. Role based access limits the scope and access the users have to information in VIRP.

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

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. NARA guidelines as stated in RCS 10-1 records retention schedule requires retention for 75 years after a program terminates.

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.

VHA Records Control Schedule (RCS 10-1) has been approved by NARA.

SORN 121VA10P2 states the records will be disposed of in accordance with General Records 5.2, item 020. GRS 5.2 provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes. The SORN is referring to RCS 10-1 prior to the revision released January 2016. Under the new RCS 10-1, referencing the General Records Schedule (GRS) crosswalk in appendix 2, the disposition is as follows:

3. Output Records.

Output records are records derived directly from the system master record. Examples include system generated reports (in hardcopy or electronic format), online displays or summary statistical information, or any combination of the above. By contrast, reports created using system information but not created directly from the system itself are not system output records, for example an annual report that agency staff prepares based on reviewing information in the system.

EXCLUSION 1: Query results or electronic reports created for a specific business need such as an established reporting requirement or a response to a formal request from a higher-level office of the agency or an entity external to the agency. Such records should be filed with an appropriate related series when applicable. If not applicable, these records must be scheduled.

EXCLUSION 2: Any hard copy records printed directly from the electronic systems that are not described below. Such records should be filed with an appropriate related series when applicable. If not applicable, these records must be scheduled.

a. Ad hoc reports. Reports derived from electronic records or system queries created on an ad hoc, or one-time, basis for reference purposes or that have no business use beyond immediate need. This item includes ad hoc reports created from or queries conducted across multiple linked databases or systems.

Temporary; destroy when business use ceases. (DAA-GRS-2013-0001-0005, item 030)

EXCLUSION 1: Reports created to satisfy established reporting requirements (e.g. statistical reports produced quarterly in accordance with an agency directive or other regular reports to management officials).

EXCLUSION 2: Records containing substantive information, such as annotations, that is not included in the electronic records. (Reports that contain substantive information should be disposed of in accordance with a NARA-approved schedule that covers the series in which they are filed.)

b. Data outputs files. Data files or copies of electronic records created from databases or unstructured electronic records for the purpose of information sharing or reference, including: • Data files consisting of summarized or aggregated information (See exclusions) • Electronic files consisting of extracted information (See exclusions) • Print files (electronic files extracted from a master file or database without changing it and used solely to produce hard-copy publications and/or printouts of tabulations, ledgers, registers, and statistical reports) • Technical reformat files (electronic files consisting of copies of a master file or part of a master file used for information exchange) (See exclusions)

Temporary; destroy when business use ceases. (DAA-GRS-2013-0001-0006, item 031)

EXCLUSION 1: Data files that are created as disclosure-free files to allow public access to the data.

EXCLUSION 2: Data files consisting of summarized information from unscheduled electronic records or records scheduled as permanent but that no longer exist or can no longer be accessed.

EXCLUSION 3: Data extracts produced by an extraction process which changes the informational content of the source master file or database.

EXCLUSION 4: Technical reformat files created for transfer to NARA.

EXCLUSION 5: Data extracts containing Personally Identifiable Information (PII). Such records require additional tracking and fall under GRS 4.2, item 15a (DAA-GRS-2013-0007-0012).

[NOTE: not media neutral. Applies to electronic records only.]

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

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. 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

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 VIR/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.

3.6 <u>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.

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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:
<u>Privacy Risk:</u> 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.

<u>Mitigation:</u> 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 by the determined method as described in VHA Records Control Schedule (RCS 10-1). 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. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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.

VIRP receives information from the sources outlined in the table below for use in the following health registries: • Breast Care Registry (BCR) • Embedded Fragment Registry (EFR) • VA Eye Injury Data Store (EIDS) • Multiple Sclerosis Surveillance Registry (MSSR) • Oncology Tumor Registry (OncoTrax) • Traumatic Brain Injury (TBI) Registry • Airborne Hazards and Open Burn Pit (AHOBPR) • Kidney Disease Registry (KDR) • Hearing Registry (HR) • Amputee Registry (AR) • Transplant Registry (TR)

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 data element types such as PII/PHI that are shared/received 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.

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Master Person Index (MPI)	To validate patient identifying data and mappings between patient identifiers, such as electronic data interchange personal identifier (EDIPI) and Integration Control Number(ICN).	Patient identifying data and mappings between patient identifiers, such as electronic data interchange personal identifier (EDIPI) and Integration Control Number (ICN).	Web Service: Simple Object Access Protocol (SOAP) XML
Veterans Health Information Systems Technology Architecture (VistA)	Utilized for analysis and research to enhance patient population care	Patient electronic health record, may include: • 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	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 • Date of Death • Last Service Separation Date • Patient EDIPI • Laboratory results • Marital Status	Structured Query Language (SQL) Server Integration Services (SSIS).
Data Access Services (DAS)	DAS sends registry records to DoD	• Name • Social Security Number • Date of Birth • Gender • Military Branch Name • Patient AHOBPR Questionnaire	Web service: RESTful, PDF
Enterprise Veterans Self Service (EVSS)	Provides gateway for veterans and service members to access the AHOBPR web application	Patient EDIPI	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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
VA Enterprise Messaging Infrastructure (eMI)	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 • OEF/OIF service indicator • Date of Death • Last Service Separation Date • Patient EDIPI • Laboratory results • Marital Status	Structured Query Language (SQL) Server Integration Services (SSIS). Web services to manage and execute the Extract, Transform, and Load (ETL) packages
Enterprise Military Information System (eMIS)	eMIS provides Person demographic, contact, military service and other benefits information including benefits eligibility profile	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 • Laboratory results • Marital Status	Structured Query Language (SQL) Server Integration Services (SSIS).

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
Privacy Risk: 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.

Mitigation: 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: This question is #7 in the Privacy Threshold Analysis.

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

VIRP receives information from the sources outlined in the table below for use in the following health registries:

- Breast Care Registry (BCR)

- Embedded Fragment Registry (EFR)

- VA Eye Injury Data Store (EIDS)

- Multiple Sclerosis Surveillance Registry (MSSR)

- Oncology Tumor Registry (OncoTrax)

- Traumatic Brain Injury (TBI) Registry

- Airborne Hazards and Open Burn Pit (AHOBPR)

- Kidney Disease Registry (KDR)
- Hearing Registry (HR)
- Amputee Registry (AR)
- Transplant Registry (TR)

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 data element types such as PII/PHI that are shared/received 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)	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, OEF/OIF service indicator, date of death, last service, Separation date, patient EDIPI. Lab results, Marital status	VA-DOD MOU. Also, Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act."	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 is the business flow	Name, Social Security number, Date of Birth, Mailing address, zip code, phone number,	VA-DOD MOU. Also, Title 38, United States Code, section 81 11	Secure electronic transfer via Hypertext Transfer

	for data between VA & DOD	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	(38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act	Protocol Secure (HTTPS), Web services to manage and execute the Extract, Transform, and Load (ETL) packages
DOD Embedded Fragment Analysis Laboratory	This is 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, OEF/OIF service indicator, date of death, last service, Separation date, patient EDIPI. Lab results, Marital status	VA-DOD MOU. Also, Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency	Secure electronic transfer via Hypertext Transfer Protocol Secure (HTTPS), Web services to manage and execute the Extract, Transform, and Load (ETL) packages

			Agreements," also known as the "Economy Act	

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

To protect veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:
1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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

Follow the format below:
Privacy Risk: 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.

Mitigation: 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 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 Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:
The System of record Notice (SORN) – National Patient Databases, 121VA10P2. The SORN can be found online at: https://www.govinfo.gov/content/pkg/FR-2018-02-12/pdf/2018-02760.pdf

121VA10P2 states 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.

1.) This Privacy Impact Assessment (PIA) also serves as notice of the PITC Insurance Payment 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."

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

In accordance with Data Use and Reciprocal Support Agreement (DURSA), depending on the information required, some data collection is mandatory while others are voluntary. For health care operations, individuals do not have to consent to use of his/her data. If the data would be used for health research, individuals would either consent to the use of his/her data or an Institutional Research Board could allow for a HIPAA waiver of authorization.

VHA Directive 1605.01 'Privacy and Release Information', section 11 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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

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

VHA permits individuals to agree to the collection of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing or sharing PII and PHI. 121VA10A7 states that individuals who wish to contest information in 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.

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: There is a risk that members of the public may not have been notice that the VIRP system exists within the Department of Veterans Affairs. Additionally, there is a risk Veterans may not have been given notice of the collection of their information in the VIRP system.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Impact Analysis and the System of Record Notice.

The VIRP system does not collect information directly from the public. Therefore, notice prior to collection would be given at the collection points of the source systems supplying data to VIRP.

SORN 121VA10A7 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?

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.

The VHA Notice of Privacy Practices informs Veterans of their right to obtain copies of their PII maintained in VHA records. Each VHA Privacy Act system of records notice (SORN) informs individuals how to obtain access to records maintained on them in the SORN. VHA permits individual to obtain access to or get copies of their PII, and this is outlined in VHA policy. Individuals must provide a written request for copies of their records to the VHA facility Privacy Officer for medical records or the System Manager for the Privacy Act system of records as outlines in the notices. The request will be processed by VHA within 20 workdays.

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.

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.

"SORN 121VA10A7 states that Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems

(10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780

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.

SORN 121VA10A7 states that Individuals seeking information regarding access to and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–6780.

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.

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

Formal redress procedure is listed in SORN 121VA10A7 as stated above in section 7.3.

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

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

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 individual may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation: By publishing this PIA and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on VIRP. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

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.

Local VHA site Veterans Integrated Registries Platform designee(s) submit an ePAS request for new application user's Veterans Health Information Systems and Technology Architecture (VistA) System account and the new application user have completed the Talent Management

System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training. Local VHA site OI&T is responsible to complete the ePAS request.
OI& Technical staff: ePAS approval for System Administrator, Application Administrator, VistA Management permission. Talent Management System (TMS) Inform Security for IT Specialist, Information Security for System Admin, Elevated Privileges for System Access, and VA Privacy and Information Security Awareness and Rules of Behavior Training.
Non-Mail enabled account (NMEA) and associated token (USB/OTP) to access the servers

Note: 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.

Continuity of the security requirements below will be met by the VIRP framework, which will contain three 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.

VIRP infrastructure will be provided by Austin Information Technology Center (AITC). Once a user gains access to the VA network, authentication will use Windows Authentication against the VA's Active Directory servers to authenticate the user against the VIRP. The VIRP framework will include a custom role-based authorization module. This authorization module will store user accounts in the SQL database. Each user account can be granted one or multiple roles such as Database administrator, Developers etc, based on the user's role at the VA. Each role can be granted access to specific functions within VIRP, or even just a certain number of functions within a specified 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 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?

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted, :* ***01/30/2019***
2. *Whether it was a full ATO or ATO with Conditions,* ***Full ATO***

3. *The amount of time the ATO was granted for,* ***3 years***
4. *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.

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

Section 9. 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.

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.05.10 16:04:14 -04'00'

Privacy Officer, Rita Grewal

Pedro A. Epting 173803

Digitally signed by Pedro A. Epting 173803
Date: 2021.05.11 09:29:04 -05'00'

Information System Security Officer, Pedro Epting

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2021.05.25 15:16:12 -05'00'

Information System Owner, Christopher Brown

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).