Privacy Impact Assessment for the VA IT System called:

Veterans Administration Central Cancer Registry (VACCR)

Development, Security & Operations

Veterans Health Administration

Date PIA submitted for review:

May 4, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kimberly Murphy	Kimberly.Murphy@va.gov	781-331-3206
Information System Security Officer (ISSO)	J. Mark McGee	James.McGee5@va.gov	520-358-3237
Information System Owner	Jeffrey Rabinowitz	Jeffrey.Rabinowitz@va.gov	732-720-5711

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 Administration Central Cancer Registry (VACCR) receives and stores information on cancer diagnosis and treatment constraints compiled and sent in by the local cancer registry staff at each of the 132 Veterans Affairs Medical Centers that diagnose and/or treat Veterans with cancer. The information sent is encoded to meet the site-specific requirements for registry inclusion as established by several oversight bodies, including the North American Association of Central Cancer Registries, the American College of Surgeons' Commission on Cancer, and the American Joint Commission on Cancer, among others. The information is obtained from a wide variety of medical record documents at the local medical center pertaining to each Veterans Health Administration (VHA) cancer patient. The information is then transmitted to the VACCR. The information is pulled from VistA instances and is sent over HTTPS (443). Details collected include extensive demographics, cancer identification, extent of disease and staging, first course of treatment, and outcomes. Data extraction is available to researchers with VA approved Institutional Review Board studies, peer review, and Data Use Agreements.

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.   *The IT system name and the name of the program office that owns the IT system.*

   The Veterans Administration Central Cancer Registry (VACCR) is owned by the Development, Security and Operations Program Office. The ownership or control of the IT system or project falls on the Veterans Health Administration (VHA) Cancer group

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

   The business purpose of VACCR is for cancer research and analysis.

   C.   *Indicate the ownership or control of the IT system or project.*
   VACCR is owned and operated by the VA.

2. Information Collection and Sharing
   D.   *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*

   The expected number of individuals whose information will be stored will be any patient who has had a cancer diagnosis and will fluctuate depending on those diagnoses

   E.   *A general description of the information in the IT system and the purpose for collecting this information.*

The Veterans Administration Central Cancer Registry (VACCR) receives and stores information on cancer diagnosis and treatment constraints compiled and sent in by the local cancer registry staff at each of the 132 Veterans Affairs Medical Centers that diagnose and/or treat Veterans with cancer. The information sent is encoded to meet the site-specific requirements for registry inclusion as established by several oversight bodies, including the North American Association of Central Cancer Registries, the American College of Surgeons' Commission on Cancer, and the American Joint Commission on Cancer, among others.

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

The information is obtained from a wide variety of medical record documents at the local medical center pertaining to each Veterans Health Administration (VHA) cancer patient. The information is then transmitted to the VACCR. The information is pulled from VistA instances and is sent over HTTPS (443). Details collected include extensive demographics, cancer identification, extent of disease and staging, first course of treatment, and outcomes. Data extraction is available to researchers with VA approved Institutional Review Board studies, peer review, and Data Use Agreements.

G. *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.*

VACCR is operated in only one site, VAMC Washington, D.C.

3. Legal Authority and SORN
H. *A citation of the legal authority to operate the IT system.*
VACCR is under the SORN 24VA10A7 Patient Medical Records "Title 38, United States Code, Sections 501(b) and 304."

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

SORN 24VA10A7 - VA legal authority to operate does not require an update at this time.

D. System Changes
J. *Whether 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. *Whether 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.

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*
- ☐ 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)

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>
*Specify type of Certificate or License Number (e.g. Occupational, Education, Medical)

PII Mapping of Components (Servers/Database)

VACCR consists of **3** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **VACCR** 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
RockyMountain\wwwroot folder	Yes	Yes	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender/Sex, Military History/Service Connection, ICN	Research and Analysis	HTTPS (443)

RockyMountain\wwwroot\VACCR_CRS\	Yes	Yes	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender/Sex, Military History/Service Connection, ICN	Research and Analysis	HTTPS (443)
RockyMountain\wwwroot\Incoming	Yes	Yes	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender/Sex, Military History/Service	Research and Analysis	HTTPS (443)

			Connection, ICN		

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?

VistA is the only source of information. VistA contains information regarding cancer patients that is collected at various medical centers which VACCR receives. There is no need for VACCR to collect information from the individual directly. VACCR aggregates the information from sites and collects and stores for research purposes. VACCR does not create information.

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.

VACCR collects the data from 131 VistA sites and creates a central repository for cancer data for research available to researchers on a national level and does not require the collection from an individual.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

VACCR does not create information.

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?

Electronic machine text transmission from VistA, not on any paper form

1.3b 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.

VACCR does not collect information 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.

1. North American Association of Central Cancer Registries (NAACCR) software performs integrity check against data. 2. Rocky Mountain Cancer Data System (RMCDS) performs additional integrity checks more sophisticated on the data and makes corrections. 3. When RMCDS cannot resolve checks, the data is reviewed by a human to verify and perform the correction.

1.4b 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.

VACCR does not check for accuracy by accessing a commercial aggregator of information.

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

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules). 24VA10A7 Patient Medical Records – VA https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf 121VA10A7 National Patient Database - VA Current SORN List (va.gov)

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:

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: VACCR will collect Personally Identifiable Information (PII) and Protected Health Information (PHI) from VistA. 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; 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.

Name - Used for synchronization with other systems;
Social Security Number - Used for synchronization with other systems;
Date of Birth - Used for synchronization with other systems;

Personal Mailing Address - Used as patient contact information;
Personal Phone Number(s) -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;
Medical Record Number – Used for synchronization with other systems;
Gender/Sex - Used for research and analysis;
Military History/Service Connection - Used for research and analysis;
Integrated Control Number (ICN) - Used for synchronization with other systems

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.

VACCR utilizes the Rocky Mountain Cancer Data System (RMCDS) which is a Windows-based software program designed to facilitate all data entry and statistical analysis functions of a hospital cancer registry in an efficient and timely manner. This software meets national standards regarding abstracting, follow-up, basic database management functions, acceptable match/merge routines for avoiding duplicate cases, basic reports, and is capable of exporting data so that additional coding and analysis can be performed.

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.

No new records are created there is only a transfer and analysis of data within the VACCR boundary.

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?

VACCR secures data in transit through HTTPS, however the data at rest is currently secured through access control, but not encryption. The physical layers of protection for the server are in place at the VA Medical Facility.

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

VACCR does not provide any additional protection for SSNs. It is stored in clear text, but encrypted through HTTPS in transit.

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. VACCR adheres to the directives outlined in OMB Memorandum M-06-15 and M-06-16 concerning PII.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

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.

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

The criteria, procedures, controls, and responsibilities regarding access to VACCR are documented in the VACCR 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, Rick and Compliance (GRC) tool.

2.4c Does access require manager approval?

Yes, VACCR utilizes the VA tools for access creations.

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
Personal Mailing Address
Personal Phone Number(s)
Current Medications
Previous Medical Records
Race/Ethnicity
Medical Record Number
Gender/Sex
Military History/Service Connection
ICN

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.*

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)?

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?

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. [VHA Publications (va.gov)](va.gov)

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

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.

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 - https://www.va.gov/vapubs/search_action.cfm?dType=1.

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.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk that the information maintained by VACCR 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 VACCR records are cleared for destruction, VACCR 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.

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.

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*
Veterans Health Administration	Research and Analysis	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Current Medications, Previous Medical Records, Race/Ethnicity, Medical Record Number, Gender/Sex, Military History/Service Connection, Integration Control Number (ICN)	XML over HTTPS

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: 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 VACCR. 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*
N/A				

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: N/A

Mitigation: N/A

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.

VACCR does not collect PII from users directly. The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on VHA's authority to collect their private health information.

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

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

N/A

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.

N/A

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

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

The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on their right to decline to provide information. (i.e., to request a restriction).

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

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

The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on their right to consent to uses of their information.

The Notice states "To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care."

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?

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 notified that the VACCR 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 VACCR 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, the Notice of Privacy Practices.
The VACCR 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 VACCR, VistA.

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.***

The VHA Notice of Privacy Practices informs Veterans of their right to obtain copies of their PII maintained in VHA records. 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.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

N/A

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

N/A

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 request inaccurate PII be corrected or amended and a process for review to determine if correction or amendment is appropriate. The individual must submit a request in writing, specify the information that they want corrected, and provide a reason to support their request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information or health records as outlined in the Privacy Notice.

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 individual must submit a request in writing, specify the information that they want corrected, and provide a reason to support their request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information or health records as outlined in the Privacy Notice.

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 request inaccurate PII be corrected or amended and a process for review to determine if correction or amendment is appropriate. The individual must submit a request in writing, specify the information that they want corrected, and provide a reason to support their request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information or health records as outlined in the Privacy Notice.

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

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

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

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

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

Follow the format below:

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 the Notice of Privacy Practices, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on VACCR. Furthermore, this document and the SORN provide additional point of contacts for those 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?

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.

OI&T is responsible to complete a Privileged Access Security (ePAS) request.
OI& Technical staff: ePAS approval for System Administrator 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)/ CyberArk (ePAS 2) to access the servers.

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 VACCR.

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?

Users from other agencies do not have access to the VACCR system.

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.

VACCR utilizes only a System Administrator role with elevated privileges to access the system, and there are no read-only or user roles.

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

ISSO. 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 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: Yes

1. *The Security Plan Status:* Signed
2. *The System Security Plan Status Date:* 3/13/2023
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 11/28/2022
5. *The Authorization Termination Date:* 11/28/2023
6. *The Risk Review Completion Date:* 6/28/2022
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.***

Please provide response here

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)

No, VACCR 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.*

N/A, VACCR 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.

N/A, VACCR 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.

    N/A, VACCR 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).

    N/A, VACCR does not use cloud technology.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

_____

Privacy Officer, Kimberly Murphy

_____

Information Systems Security Officer, J. Mark McGee

_____

Information Systems Owner, Jeffrey Rabinowitz

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).

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

24VA10A7 Patient Medical Records – VA
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

121VA10A7 National Patient Database - VA
Current SORN List (va.gov)

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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