Privacy Impact Assessment for the VA IT System called:

Compliance Inquiry Reporting & Tracking System (CIRTS)

VHA Center for Business Integrity – (CBI)

Date PIA submitted for review:

November 9, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Takeshia Berkeley	Takeshia.Berkeley@va.gov	404-828-5337
Information System Security Officer (ISSO)	Michael Lumby	Michael.Lumby@va.gov	(407) 622-4162
Information System Owner	Robert Jacobs	Robert.Jacobs@va.gov	202-316-1855

Abstract

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

The Compliance Inquiry Reporting & Tracking System (CIRTS) application is used by Compliance Officers at each VA Medical Center to record and track the receipt and disposition of reports and/or concerns related to matters of the business integrity of VHA operations in the course of investigating allegations of compliance violations. The purpose of the CIRTS system is to establish a process to receive reports of suspected compliance violations, and to maintain a system to respond to such allegations.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Compliance Inquiry Reporting & Tracking System (CIRTS) server and associated software application is physically located at the Health Resource Center (HRC) and is managed by Tier III server support personnel. Minimal local support is provided by the Eastern Kansas Area OI&T staff. The CIRTS application is used by Compliance Officers (approximately 200-300 users total) at each VA Medical Center. The CIRTS system is established to control the receipt and disposition of reports and/or concerns related to the following VHA areas: Enrollment; Means Testing; Eligibility; Pre-certification and certification/utilization review; Standards pertaining to documentation, coding and billing; Audits, reviews, inquiries and remediation; Accounts receivable and payable; Excluded individuals and/or entities screening and sanctions listings; Information protection, record retention, managing requests for information; Provider documentation supporting business processes; Overpayments; Questionable

conduct on the part of managers, supervisors or employees as related to business processes; and any other matter relating to the business integrity of VHA operations.

Information in the CIRTS system is not shared with any other VA system or entity. VHA Office of Integrity and Compliance has the same responsibility and requirement that all VA employees have to report instances of waste fraud and abuse that are discovered in the course of investigations to the VA Office of the Inspector General (OIG).

The System of Records governing CIRTS is 110VA17 "Compliance Record, Response, and Resolution of Reports of Persons Allegedly Involved in Compliance Violations—VA".

The legal authority to operate the IT system is Title 38 USC Section 501, Title 38 USC 7332, and 45 CFR Parts 160 and 164.

Information is collected by Compliance Officers and then data entry is performed directly via Client / Server application interfaces. Only OICOIC Program Office personnel and Compliance Officers have access to enter data into the system. OICOIC Program Office personnel and Compliance Officers are the only ones that will collect information. Information collected may include: (1) The name of the subject of an investigation; (2) the names of individuals whose work was reviewed as part of the investigation; (3) the names or patient numbers of Veteran patients whose medical records were reviewed in order to investigate the allegation; (4) the station at which an investigation took place; (5)the time period when the investigation took place; (6) the nature of the allegation; (7) the outcome of the investigation; (8) the recommended action; and, 9) the identification number assigned to the case. Information may be in the form of a narrative summary or synopsis, exhibits, or internal documentation and memoranda.

User accounts are created with specific privileges to the application. These accounts are controlled through credentials that are managed by the application. Access to computerized information in the database is restricted to authorized personnel on a need-to-know basis by means of passwords and authorized user identification codes. Computer system documentation will be maintained in a secure environment in the VHA Office of the Integrity and Compliance, and in the Compliance Offices at the network and medical center locations. Physical access to printouts and data terminals will be limited to authorized personnel in the Compliance Program. Access to file folders is restricted to authorized personnel on a need-to-know basis. Paper files are maintained in file cabinets or closets and are locked after duty hours. These files are under the control of the Compliance Officer or his/her designees. Buildings are protected from unauthorized access by a protective service.

CIRTS is used by OIC Officers in all VA Medical Centers, VISN Offices, and select VACO Program Offices, it is housed on the LAN at Health Resource Center (HRC) in Topeka, KS., which is under the Eastern Kansas Area for OIT support.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Information in the investigation records may include: (1) The name of the subject of an investigation; (2)the names of individuals whose work was reviewed as part of the investigation; (3) the names or patient numbers of Veteran patients whose medical records were reviewed in order to investigate the allegation; (4) the station at which an investigation took place; (5) the time period when the investigation took place; (6) the nature of the allegation; (7) the outcome of the investigation; (8) the

recommended action; and, 9) the identification number assigned to the case. Information may be in the form of a narrative summary or synopsis, exhibits, or internal documentation and memoranda.

PII Mapping of Components

This system does not connect to any internal/external system.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A					

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

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

Records (or information contained in Records) in this system include allegations made by individuals calling the VHA Office of Integrity and Compliance Help Line, or through another source, to report a possible violation of law, rules, policies, procedures, regulations, or external program requirements such as third-party payer billing guidelines. Records may also contain reports of the reviews or investigations conducted at the medical center, VISN, or Central Office level to verify the reported allegations and take remedial action as needed.

1.3 How is the information collected?

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

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

The information in this system is obtained from calls that are received through the VHA Integrity and Compliance Help Line and reports received through other sources (letters, email, fax) to report a possible violation of law, rules, policies, procedures, regulations, or external program requirements. Information is obtained from VHA employees, Veterans, third parties such as contractors, and VHA records which may include billing data, patient medical records, policies and procedures, and memoranda, and documents submitted to investigators, interviews, and from VA information systems. Records in the system will be a combination of computerized files and paper files.

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

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

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

Information contained in allegations of wrongdoing are verified or collected, in the course of investigations, from individuals and from official VA databases and systems. The nature of the investigative process itself is the collection of accurate information, verified by the official sources. Individuals are informed and aware their reports are being tracked in CIRTS for an investigation and response, and they are provided with a CIRTS reference number which indicates which report houses the data they provide.

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

Title 38 USC Sections 501, Title 38 USC 7332, and 45 CFR Parts 160 and 164

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: The CIRTS system collects both Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result.
Mitigation: CIRTS employs the standard VA required security measures for a High-Impact System designed to ensure that the information is not inappropriately disclosed or released. These security measures are specified in the controls VA Handbook 6500 "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program".

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 to identify the patient during appointments and in other forms of communication.

•**Social Security Number:** Used as a patient identifier and as a resource for verifying income information with the Social Security Administration.
•**Date of Birth:** Used to identify age and confirm patient identity.
•**Personal Mailing Address:** Used for communication, billing purposes and calculate travel pay.
•**Personal Phone Number(s):** Used for communication, confirmation of appointments and conduct telehealth appointments.
•**Personal Fax Number:** Used to send forms of communication and records to business contacts, insurance companies and health care providers.
•**Personal Email Address:** Used for communication and My HealtheVet secure communications.
•**Emergency Contact Information** (Name, Phone Number, etc. of a different individual): Used in cases of emergent situations such as medical emergencies.
•**Financial Account Information:** Used to calculate co-payments and VA health care benefit eligibility.
***Name of the Subject of an Investigation**
***Name of Individuals who work was reviewed as part of the investigation**
***Name or patient numbers of those who medical records were reviewed**
***Station at which investigation took place**
***Time Period of Investigation**
***Nature of Allegation**
***Outcome of Investigation**
***Recommended Action**
***Case Identification Number**

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

Statistical information that does not included individual SPI is aggregated for internal reports as needed. OIC Internal Reports are being generated from CIRTS including roll up data of OIC Helpline Reports to evaluate VHA risk areas with high levels of reports. This information is not specific in nature, and rolls-up risk information by subject category without PHI/PII information. This information is reported internally to Compliance committees and OIC management. OIC Officers in the field could utilize CIRTS information specific to their entity to report risk areas to their leadership. However, there is no sharing of PII or SPI.

2.3 How is the information in the system secured?

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

Content Manager (CM) features a comprehensive security and Access Control system that requires 3 levels of authorization before access to a document is granted.

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

Content Manager features supplemental markings that enable this layer of security

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

Content Manager's featured supplemental markings are applied to records that contain PII and PHI and only authorized personnel within the system may access it. The access list is controlled by the system administrator via CM's Locations Feature.

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

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

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

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

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

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.

User accounts for the CIRTS application are created with specific privileges to user. These accounts are controlled through credentials that are managed by the application. Access to computerized information in the database is restricted to authorized personnel on a need-to-know basis by means of passwords and authorized user identification codes. Physical access to printouts and data terminals will be limited to authorized personnel in the Compliance Program. Access to paper file folders is restricted to authorized personnel on a need-to-know basis. Paper files are maintained in file cabinets or closets and are locked after duty hours. These files are under the control of the Compliance Officer or his/her designees.

Information is collected by Compliance Officers and entered into the CIRTS application. Only Compliance Officers will collect PII information and only Compliance Officers have access to enter data into the system.

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

All electronic data stored in the CIRTS system, and paper files, associated with the reported allegation of a VHA compliance violations and generated in the course of the investigative process. Information in the investigation records may include: (1) The name of the subject of an investigation; (2)the names of individuals whose work was reviewed as part of the investigation; (3) the names or patient numbers of Veteran patients whose medical records were reviewed in order to investigate the allegation; (4) the station at which an investigation took place; (5) the time period when the investigation took place; (6) the nature of the allegation; (7) the outcome of the investigation; (8) the recommended action; and, 9) the identification number assigned to the case. Information may be in the form of a narrative summary or synopsis, exhibits, or internal documentation and memoranda. PII and SPI that is retained in the system is individual name, SSN, DOB, mailing address, phone numbers, fax number(s), email address, emergency contact information (name, phone number, etc of a different individual), used to identify and contact individuals, and financial account information, current medications if needed in the course of an investigation.

3.2 How long is information retained?

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

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

According to the VHA System of Records Notice (SORN) 110VA17 "Computerized records will be retained indefinitely. Periodic system back-ups will be employed for record protection. If disk space is limited, the records will be archived to tape or disk in accordance with established practice."
Paper records will be maintained and disposed of in accordance with VHA Records Control Schedule (RCS 10-1) as authorized and approved by the Archivist of the United States.

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.

Yes. CIRTS uses the VHA Records Control Schedule RCS 10-1.
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

There is no specific retention schedule for CIRTS. A request to NARA for a CIRTS specific retention schedule is in process. Until a retention schedule has been provided, CIRTS data is not being destroyed. It is maintained indefinitely in the CIRTS database and no data is purged.

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

Please see SORN 110VA17: Federal Register :: Privacy Act of 1974; System of Records

Electronic records are not destroyed or eliminated. Paper records at the end of their retention period that are eligible for destruction are destroyed by shredding. The shredding company is determined by the shredding contract at facility where each respective OIC office is located, and all documentation regarding shredding is controlled by that facility as one entity.

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

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

Information is not repurposed for any other reasons.

3.6 <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:
Privacy Risk: The risk to maintaining data within the CIRTS system is the longer time frame information is kept, the greater the risk that information possibly will be compromised or breached.
Mitigation: CIRTS collects only data necessary for investigating allegations of wrongdoing. Information is collected by Compliance Officers and entered into the CIRTS application. Only Compliance Officers have access to the system. Access to computerized information in the database is restricted to authorized personnel on a need-to-know basis by means of passwords and authorized

user identification codes. The only other access to CIRTS is by System Administrators on the HRC OI&T staff for system administration, maintenance and management.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

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

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

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

Follow the format below:
Privacy Risk: There is a risk that information may be shared with unauthorized VA program or system or that data could be shared.
Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need to know basis, PIV Cards, PIN numbers, encryption, and access authorization are all measures that are utilized within the facilities.

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: There is a no risk that information may be shared with an external organization or agency that does not have a need or legal authority to access VA data.
Mitigation: There is no file sharing with external entities. OIC Follows VHA HB 1605.1, "Privacy and Release of Information" in regard to external sharing. The Freedom of Information Act (FOIA) exempts CIRTS records from mandatory disclosure. FOIA Exemption 6 exempts from mandatory disclosure personnel, medical, and other files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. As CIRTS information is filed and retrieved under the individual's case # or name, the individual has a first party right of access to obtain a complete un-redacted copy in most situations. Exemption 7 protects records or information compiled for law enforcement purposes.

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.

Yes. For OIC Helpline purposes, individuals are informed and aware their reports are being tracked in CIRTS for an investigation and response, and they are provided with a CIRTS reference number which indicates which report houses the data they provide. OICOs and Liaisons in the field conducting investigations notify appropriate individuals of the information necessary to proceed with the investigation. VA also provides notice to Veterans and their dependents on what information is collected on them and what that information is used for. This notice is provided in the Notice of Privacy Practices VA 10-163. Link provided in the appendix.

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

Yes, In the midst of an investigation an individual may decline to provide information. A penalty or denial of service is not attached; however, the denial of information is documented in CIRTS to provide a paper trail of workflow. In this event if fraudulent activity is suspected and OIC's investigation is halted, OIC notifies VA OIG of the reported allegation for action as needed.

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

There are no particular uses of CIRTS data that necessitate consent. As information in the CIRTS system is not shared with, or accessible by, any other entity, PHI/PII/SPI is not compromised.

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 veterans and other members of the public will not know that the CIRTS exists or that it collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.
Mitigation: Individuals are informed and aware that identifying information they provide is tracked in CIRTS for an investigation and response, and they are provided with a CIRTS reference number which indicates which report houses the data they provide. There are no particular uses of CIRTS data to necessitate consent. PHI/PII is not being compromised.

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.

CIRTS is a Privacy Act system of records and is subject to FOIA processes. The Office of Integrity and Compliance maintains a toll-free Helpline for Veterans, employees, or the general public to anonymously (if desired) report potential acts of wrongdoing or violations of VHA policies or procedures. The OIC Helpline may be contacted at (866) 842-4357 (VHA-HELP) or via email at VHAOICHelpline@va.gov.

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

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

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

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are provided with a CIRTS reference number which indicates which report houses the data they provide. An individual who seeks access to or wishes to contest records maintained under his or her name in this system may write, call or visit the VHA Office of Integrity and Compliance (10B3) Department of Veterans Affairs, 810 Vermont Avenue, NW. Washington, DC 20420. 202-745-8000 Ext. 55533.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

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

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

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

Mitigation: Individuals are informed and aware that identifying information they provide is tracked in CIRTS for investigation and response purposes. An individual may file a Privacy Act request and Freedom of Information Act (FOIA) request for information about them. Privacy Act and Freedom of Information Act requirements are followed in providing this information to an individual. CIRTS data is not routinely shared with other entities and there is no access to the CIRTS system outside of OIC Compliance Officers and OI&T System Administrators.

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.

Only OIC Compliance Officers have access the CIRTS system. No other individuals or persons have access to the CIRTS system or information, except for OI&T System Administrators for the purposes of computer system administration, management and maintenance. Active Directory accounts identify individuals in the authorized CIRTS user group. User accounts for the CIRTS application are created with specific privileges to the user. These accounts are controlled through credentials that are managed by the CIRTS application. Access to computerized information in the database is restricted to authorized personnel on a need-to-know basis by means of passwords and authorized user identification codes. Physical access to printouts and data terminals is limited to authorized personnel in the Compliance Program. Access to paper file folders is restricted to authorized personnel on a need-to-know basis. Paper files are maintained in file cabinets or closets and are locked after duty hours. These files are under the control of the Compliance Officer or his/her designees at the respective OIC locations.

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 contractors have access to CIRTS system or data.

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.

The TMS course "VA Privacy and Information Security Awareness and Rules of Behavior" is an annual VA requirement.

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

If Yes, provide:

1. *The Security Plan Status, Approved*
2. *The Security Plan Status Date, 9/20/21*
3. *The Authorization Status, Authorization to Operate (ATO)*
4. *The Authorization Date, 12/17/20*
5. *The Authorization Termination Date, 12/17/21*
6. *The Risk Review Completion Date, 11/9/21*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH). Moderate*

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 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

N/A

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

N/A

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

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

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

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.

TAKESHIA BERKELEY

Digitally signed by TAKESHIA BERKELEY
Date: 2021.11.30 11:48:23 -05'00'

Privacy Officer, Takeshia Berkeley

MICHAEL D. LUMBY 157768

Digitally signed by MICHAEL D. LUMBY 157768
Date: 2021.11.30 11:41:20 -05'00'

Information Security Systems Officer, Michael Lumby

Robert B Jacobs 573866

Digitally signed by Robert B Jacobs 573866
Date: 2021.11.30 12:32:51 -07'00'

System Owner, Robert Jacobs

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).

VHA Notice of Privacy Practices:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8928