Privacy Impact Assessment for the VA IT System called:

# Radiotherapy Incident Reporting and Analysis System (RIRAS)

## National Radiation Oncology Program Office

## VHA National Radiation Oncology Program (11SPEC22)

Date PIA submitted for review:

2022/01/18

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Grewal, Rita | Rita.Grewal@va.gov | (202)632-7861 |
| Information System Security Officer (ISSO) | Kehinde Talabi | Talabi.Kehinde@va.gov | (202)632-7464 |

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Information System Owner | Rabinowitz Jeffrey | 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.*

This Web application is designed to collect Radiation Oncology profile data, facility credentialing status, facility accreditation status, incident reports and quality monitoring data.
Capital Region Readiness Center (CRRC)

## 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 VHA National Radiation Oncology Program (10P4H) own and maintains the Radiotherapy Incident Reporting and Analysis System (RIRAS) on its VA intranet Web-based module that is designed as a comprehensive solution for documenting, tracking, and analyzing patient safety related incidents in radiation oncology services within the Veterans Health Administration. It is an important facet of the continuing effort by the National Health Physics Program (NHPP) and the National Radiation Oncology Program (NROP) to maintain and improve radiotherapy safety. A key attribute of the VHA-RIRAS is strong confidentiality protections to the radiation oncology facilities and healthcare providers who report adverse events and incidents.

RIRAS is fully compliant with the patient safety act and has following attributes:

- Collection and analysis of patient safety incidents: Web-based electronic infrastructure is used to collect and aggregate adverse event and "good catch" (near miss) data from all VHA radiation oncology services (ROS).

- Development and dissemination of information with respect to improving patient safety: The RIRAS has utilities that provide a corrective action plan for each event reported by the ROS. The feedback to the ROS includes recommendations for mitigating future errors, protocols for safe operations, and information regarding best practices. The threshold for events that require a corrective action plan is developed by the NROP/NHPP.

- Use patient safety work products to encourage a culture of safety and to provide feedback and assistance to effectively minimize patient risk: The de-identified aggregated data collected by the RIRAS is used to develop safe standard operating procedures for each radiotherapy treatment modality and technique.

- Maintenance of procedures to preserve confidentiality with respect to patient safety work product: The event reported data do not contain any patient health information/personally identifiable information (PHI/PII). However, the data reported by ROS do include facility facility data, which are used to investigate the reported event. The facility data (radiation oncology facility and provider information) is purged as soon as the data are analyzed by the NHPP/NROP team. Therefore, the adverse event/incident data stored in the RIRAS are completely de-identified.

- Improvement to patient safety and the quality of health care delivery of patients treated with radiotherapy: The electronic infrastructure of the RIRAS is used to collect and aggregate event data from ROS. The radiation oncology domain expert staff at NROP analyzes each reported event and determines its cause and severity. The de-identified aggregated data are analyzed to evaluate population-based trends, which in turn is used to improve the safety and quality of radiotherapy.

Expected Number of Individuals whose Information is Stored in the Solution

- RIRAS only collects information of adverse events and "good catches" for patients treated in Radiation Oncology.

General Description of Information Stored in the IT System

- Gather and maintain Radiation Oncology Services (ROS) profile data: These data will contain information about the facility demographic, services provided, patient volume, details on radiation treatment planning and delivery equipment, quality assurance activities, staff credentials, etc. Data will be captured via web-based forms and data elements used in this form would have interdependencies between them. We will be able to perform advanced analytics on the types of services, volume of patients, equipment usage, etc., using these data.

- Gather information on the accreditation and credentialing status of each ROS: These data will be collected and updated periodically via web-based forms. We will be able to perform queries on these data and pertinent automatic alerts via email will be generated to inform ROS staff about their accreditation and credentialing status.

- Create a system-wide log of machine Quality Assurance (QA) periodic remote monitoring of output data and provide each ROS a feedback on a continuous basis. Each facility will have an ability to compare their data with the aggregated data from all other facilities.

- Radiotherapy Incident Reporting and Analysis system (RIRAS) collects adverse medical event/incident data, which are deidentified before it is stored in the database RIRAS collects adverse medical event/incident data, which are deidentified before it is stored in the database. This system has utilities that provide a corrective action plan for each adverse event/incident reported by the ROS. The feedback to the provider will include recommendations for mitigating future errors, protocols for safe operations, and information regarding best practices. The de-identified aggregated data collected by the RIRAS system will be used to develop safe standard operating procedures for each radiotherapy treatment modality and technique. The event reported data will not contain any patient PHI/PII.

System Operation - Control of PII

- The system is physically installed in one location. The system is accessed by a common website available to all 40 radiation oncology clinics.

Information Sharing

- There are two VHA internal organizations that have "Staff" access – (1) the National Health Physics Program (NHPP) - and - (2) the National Radiation Oncology Program (NROP.) "Staff" access provides access to all data in the system

Legal Authority

- Required by Federal Law (10 CFR 34.3045)
- VHA Directive 2013-007

## 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)

A unique facility specific number assigned to each event that is reported in RIRAS.
This number is used by NHPP/NROP to communicate with ROS while the adverse event/incident is under active analysis. However, this number is purged from the database at the completion of adverse event/incident analysis

Note:
(1) Name ("Full Name") and e-mail address ("E-mail") are collected for an Individual who is a "Registered Reporter." A "Registered Reporter" is always a VA Employee or a VA Contractor. These fields are not collected for Veterans

**PII Mapping of Components**

Radiotherapy Incident Reporting and Analysis System (RIRAS) consists of one key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by RIRAS and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

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

*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** |
|---|---|---|---|---|---|
| NROPA | Yes | Yes | Fullname | Though the system is integrated with VA SSOi, the software keeps track of the activity logs and records the reporters names, email address to reach out in case there is a follow-up required with a particular report. | Full name field in the RIRAS DB is stored in an encrypted format |
| NROPA | Yes | Yes | Email | The reporters VA email address is recorded in the RIRAS DB to send out auto emails and notifications with updates to their reported events. | Email field in the RIRAS DB is stored in an encrypted format |

### 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.*

VA Radiation Oncology services will use this system and enter adverse events /incident data. The designated staff at NHPP/NROP that has patient safety experience in radiation oncology domain will perform analyses of these reported events.

### 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.*

VA Radiation Oncology services will use the electronic system and enter adverse event/incident data. The data submitting service will either create a registered account in RIRAS and then enter data in the electronic event report form or report an event anonymously. The event data are collected on a web browser and the website is deployed on the VA intranet.

### 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.*

RIRAS is developed to meet the requirements for mandatory reporting of medical events in radiation oncology outlined in Federal Law (10 CFR 34.3045) and VHA Directive 2013-007 "Mandatory Reporting for Misadministration's of Therapy Machine Sources of Ionizing Radiation". The events reported in RIRAS are reviewed and analyzed by the NHPP & NROP. Once the root cause analysis is completed by NHPP/NROP, the data is de-identified (RT number, radiation oncology facility and provider information purged) before it is stored in the database. The events that will be reported anonymously do not contain RT number, radiation oncology facility and provider information data fields.

**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*

RIRAS solution complies with the Federal Law (10 CFR 34.3045) and VHA Directive 2013-007 that establishes mandatory reporting for misadministration's of therapy machine sources of ionizing radiation. The Food and Drug Administration (FDA) also hosts an adverse event reporting system called FAERS but reporting in that system is voluntary.
VA Privacy Service Current SORN List (va.gov) *99VA13/74 FR 14613* - Automated Safety Incident Surveillance and Tracking System-VA.

**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:*

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

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

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

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

Follow the format below when entering your risk assessment:
**<u>Privacy Risk:</u>**
The event reporter from ROS may include PHI/PII data in the free text fields of the event reporting form.

**<u>Mitigation:</u>**
Each reported event is reviewed and critically analyzed by NHPP/NROP. Therefore, any PHI/PII data reported in the free text fields will be scrubbed by the NHPP/NROP analyst.

## 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.*

- Gather and maintain Radiation Oncology Services (ROS) profile data: This data will contain information about the facility demographic, services provided, patient volume, details on radiation treatment planning and delivery equipment, quality assurance activities, staff credentials, etc. Data will be captured via web-based forms and data elements used in this form would have interdependencies between them. We will be able to perform advanced analytics on the types of services, volume of patients, equipment usage, etc.; using these data.

- Gather information on the accreditation and credentialing status of each ROS: These data will be collected and updated periodically via web-based forms. We will be able to perform queries on these data and pertinent automatic alerts via email will be generated to inform ROS staff about their accreditation and credentialing status.

- Create a system-wide log of machine QA periodic remote monitoring of output data and provide each ROS a feedback on a continuous basis. Each facility will have an ability to compare their data with the aggregated data from all other facilities.

- RIRAS collects medical adverse event/incident data, which are de-identified before it is stored in the database. This system has utilities that provide a corrective action plan for each event reported by the ROS. The feedback to the provider will include recommendations for mitigating future errors, protocols for safe operations, and information regarding best practices. The de-identified aggregated data collected by the RIRAS system will be used to develop safe standard operating procedures for each radiotherapy treatment modality and technique. The adverse event/incident reported data will not contain any patient health information (PHI).

### 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*

NHPP / NROP will analyze each adverse event/incident reported by the ROS. The feedback to the provider will include recommendations for mitigating future errors, protocols for safe operations, and information regarding best practices. The system has tools to display aggregate number of events in discrete process steps in graphs and textual format. The aggregated data are analyzed to evaluate population-based trends, which in turn will be used to improve the safety and quality of radiotherapy within VHA.

### 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?*

All data in transit is protected via the SSL certificates. The PII data fields within the SQL database are encrypted

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

We do not collect SSNs in the RIRAS application.

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

N/A

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

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

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

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

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

*<u>Principle of Use Limitation:</u> Is the use of information contained in the system relevant to the mission of the project?*

*This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.*

Add answer here:

Each reported incident includes age, gender, and the unique facility specific number. All these data elements are stored in an encrypted format in the RIRAS database. This information is necessary for the NHPP/NROP staff to analyze each reported incident. As soon as the incident analysis is completed, a patient safety work product is generated, which does not include these data elements. Therefore, for all incidents for which the analysis is complete, the RIRAS database does not have any data that can either identify a patient for whom the event is reported or the ROS.

## 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*

No Patient PHI/PII information is retained by the system. After the analysis is complete on the incident, all ROS-specific data are purged before it is stored in the database.

For Registered Reporters (always a VA Employee or a VA Contractor) – the name and e-mail address is retained.

**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.*

Each reported incident includes age, gender, and the unique facility specific number are retained in the database till the analysis is completed on the reported adverse event/incident. All these data elements are stored in an encrypted format in the RIRAS database. The anticipated timeframe for complete analysis is four weeks. As soon as the analysis is completed, the aforementioned patient and ROS-specific data are purged from the adverse event/incident reporting form before it is stored in the database.

For **Registered Reporters,** the name and e-mail address are retained for the retention period required under departmental rules for events under their domain.

These records are retained and disposed of after 3 years in accordance with the National Archives and Records Administration Schedule 10-1, section 1150.3 (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf) and 10 CFT 36.81 (https://www.nrc.gov/reading-rm/doc-collections/cfr/part036/part036-0081.html)

**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.*

Not applicable for Patient information because no PHI/PII data are stored in the database for Patients.

For Registered Reporters, the name and e-mail address are retained for the retention period required under departmental rules for events under their domain.

These records are retained and disposed of after 3 years in accordance with the National Archives and Records Administration Schedule 10-1, section 1150.3 (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf) and 10 CFT 36.81 (https://www.nrc.gov/reading-rm/doc-collections/cfr/part036/part036-0081.html)

**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*

Not applicable for Patient information because no PHI/PII data are stored in the database for Patients.

For Registered Reporters, the name and e-mail address are retained for the retention period required under departmental rules for events under their domain.
No Patient PII data is retained in the record.

**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*

Not applicable - No patient PII

### 3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.*

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

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

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

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

Follow the format below:
**Privacy Risk:** None (for patients)
For Registered Reporters: the name and email address information are retained in the software
For Patients – No PII/PHI is asked to be reported in the RIRAS form templates but might be entered in the free-text fields to describe the event.

**Mitigation:**
For Registered Reporters: The name and email address are recorded at the time of account registration in the RIRAS software. This information is available on the VA- Active directory system under the VA's outlook address book. This information is available to anyone who has access to the VA network and hence there is minimal privacy risk to store this information in the RIRAS database. This information is retained till the users account is active in the system.

For Patients: No Patient PHI/PII information is asked to be reported in the RIRAS form templates but incase a reporter enters this information in the free-text fields then these are redacted by the subject matter expert reviewers when they are analyzing the events. The subject matter expert analysis of the data in done every week and hence we do not anticipate any PHI/PII information entered in the free-text fields of the report stored in the database for more than one week. The subject matter expert reviewers have been educated to look for any PII/PHI elements in the reports and redact them when found. The reporters have been instructed to not include any PHI/PII elements in the reports.

## 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.*

Incident reports will be jointly reviewed and analyzed by the NHPP and the NROP. The NROP Office provides the subject matter expertise in radiation oncology domain.

*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*** |
|---|---|---|---|
| Both NHPP/NROP have access with password protection to each reported incident via intranet | To analyze reported incidents | Adverse event/" good catch" information reported by radiation oncology services. Staff name, email address and facility for each user | Web portal |

| ***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*** |
|---|---|---|---|
| Web portal. This information will be located behind a VA firewall. | | | |

**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:

**<u>Privacy Risk:</u>**

Access to the RIRAS software for individuals who is not authorized to view and report the reports.

**<u>Mitigation:</u>**

RIRAS is integrated with the VA's SSOi and information is only accessible to authorized individuals to enter and view the reports in the system.

## Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

*Data Shared with External Organizations*

| ***List External Program Office or IT System information is shared/received with*** | ***List the purpose of information being shared / received / transmitted with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system*** | ***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)*** | ***List the method of transmission and the measures in place to secure data*** |
|---|---|---|---|---|
| N/A | N/A | N/A | N/A | 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:**
None; only de-identified population-based data will be reported on the RIRAS Website for other users who are registered within the RIRAS database to view. No user outside the approved RIRAS group are allowed to access any data within the RIRAS database.

**Mitigation:**
Not applicable

## 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.*

VA Privacy Service
Current SORN List (va.gov) *99VA13/74 FR 14613*
Automated Safety Incident Surveillance and Tracking System-VA.

**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*

Not applicable, This is a voluntary reporting system and there is no penalty for VA employees to not reporting in this system.

**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*

Not applicable, this is a voluntary reporting system, and the use of the reported information is for provide feedback / mitigation strategies/ learning actions for the reported event and guidance for preventing such events from happening in the future. The purpose and use of the reports is clearly spelled out in the informational pages of the RIRAS web pages.

### 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:**
None

**Mitigation:**
Not applicable

## 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.*

RIRAS aggregates data on adverse events/incidents reported by the ROS. Even though, reported data are in reference to veterans treated at that ROS yet there is no veteran-specific data in the RIRAS database. The reporters will have access to their reports and only to population-based adverse event/incident statistics. Please note that any adverse event/incident that results in harm to a patient is reported separately to the patient safety office.

**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.*

All reports are analyzed by subject matter experts because further analysis is completed. Any discrepancies or inaccurate information is sent back to the reporters for correction before the analysis is completed.

**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.*

The RIRAS software enables the reports to be sent back to the reporters via the subject matter expert (SME) reviewers. Email notifications are sent to the reports informing them that amendments in the reports are required before resubmission for further completing the review.

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

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

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

Not applicable, RIRAS does have a mechanism where the SME can request for the reports to be corrected and resubmitted.

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

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

*Consider the following FIPPs below to assist in providing a response:*
*<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:
**<u>Privacy Risk:</u>**

There are no known privacy risks with the current workflow where every report is carefully analyzed by the SME to have the reporter correct for any inaccurate or erroneous information.

**Mitigation:**
Not applicable

## 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.*

RIRAS team at NROP/NHPP ensures strict access to information and hosting environments by enforcing thorough access control and requirements for reporter using this system. As a part of our access management activities, the following security capabilities are in place: multi-factor authentication, individual administrator user-ids and access based on need, maintaining minimum password strength, disabling users on five incorrect password attempts and maintaining user logs. In addition, we have implemented SSL on the website so all the network traffic will be encrypted.

The following user access roles are created as a part of the RIRAS system.

| | |
|---|---|
| Facility Admin | Authorized to enter incident/events, update facility profile and view events reports from the designated facility. |
| Facility Reviewer | Authorized to only view incident/events reports. Not allowed to update facility<br>profile or report events from the designated facility. |
| General User | Authorized to view the facility profile form and enter incidents/events from the designated facility. Only allowed to view incidents / events reported by themselves and not from the everyone in the designated facility. |
| Registered user | Users who have self-registered but not approved by the RIRAS administrator |

| | |
|---|---|
| Staff | RIRAS administrator who has access to all data from all facilities and performs analysis and generated the work product report that is sent back to the facilities. |

**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 VA contractors will have access to this system unless they are Registered Reporters – and as a Registered Reporter, they will NOT have access to PII. All the VA contractors who provide clinical physician and physicist servers to our VA medical centers have Business Associate Agreement (BAA) as part of the locally executed contract.

**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.*

All users access the RIRAS must complete VA required trainings using the Talent Management System (TMS), including:
(1) VA Privacy and Information Security Awareness and Rules of Behavior Training
(2) Privacy and HIPAA Focused Training

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

*If Yes, provide:*

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*

7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

RIRAS Security Plan Status is approved, with Security Plan Status date of October 05, 2021. An Authorization and Accreditation (A&A) has been completed and RIRAS is in continuous monitoring with a 180 Days (ATO) granted on January 18, 2022, with an expiration date of July 17, 2022, with Risk Review Completion Date of December 29, 2021. The FIPS 199 classification of the system is Moderate.

## Section 9 – Technology Usage

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

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

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

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

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

NOT APPLICABLE

**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.*

NOT APPLICABLE

**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.*

NOT APPLICABLE

**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.*

NOT APPLICABLE

**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).*

NOT APPLICABLE

## 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.**

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2022.01.27 22:27:23 -05'00'

**Privacy Officer, Grewal, Rita**

Kehinde A. Talabi 1562515

Digitally signed by Kehinde A. Talabi 1562515
Date: 2022.02.02 15:20:53 -05'00'

**Information Systems Security Officer, Kehinde Talabi**

JEFFREY RABINOWITZ 254742

Digitally signed by JEFFREY RABINOWITZ 254742
Date: 2022.02.02 13:47:33 -05'00'

**Information Systems Owner, Rabinowitz Jeffrey**

## 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).

Link to VA Privacy Website: https://www.va.gov/privacy/ .

Link to VHA Notice of Privacy Practices:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3048.