US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/02/2025

OPDIV:

NIH

Name:

Research Advocate System (RAS)

PIA Unique Identifier:

P-4190804-047456

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

Does the system include a Website or online application available to and for the use of the general public?

No

Identify the operator.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The PIA has been updated to meet the requirements of Executive Order - Defending Women From Gender Ideology Extremism And Restoring Biological Truth To The Federal Government.

Describe the purpose of the system.

National Cancer Institute (NCI) Office of Advocacy Research (OAR) Research Advocate System (RAS) allows advocates within the community to share information about their advocacy experience and expertise with National Cancer Institute's (NCI) Office of Advocacy Relations (OAR).

Describe the type of information the system will collect, maintain (store), or share.

Information collected includes contact information (including name, address, email address, phone number). The system also includes resume curriculum vitae, work experience and demographic information, sex, age (ranges, not actual ages), languages, education. Sex and demographic information all have the response option of “Prefer Not to Disclose” as well as self-reported information about interest and experience in cancer advocacy.

Users log in to this system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

National Cancer Institute (NCI) Office of Advocacy Research (OAR) Research Advocate System (RAS) allows advocates within the community to share information about their advocacy experience and expertise with National Cancer Institute's (NCI) Office of Advocacy Relations (OAR).

Information collected includes contact information (including name, address, email address, phone number). The system also includes resume curriculum vitae, work experience and demographic information, sex, age (ranges, not actual ages), languages, education. Sex and demographic information all have the response option of “Prefer Not to Disclose” as well as self-reported information about interest and experience in cancer advocacy.

Users log in to this system using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of IAM Services is to authenticate and authorize all users and computers in a Windows domain type network; assigning and enforcing information security policies for all computers and installing or updating software. The IAM Services collect unique user credentials and stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name
E-Mail Address
Mailing Address
Phone Numbers
resume/CV
work experience
personal connection to cancer
sex, age (ranges, not actual ages), demographic information, languages, education
advocacy experience and interest

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees
Public Citizens

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

Personally Identifiable Information (PII) is used by OAR and NCI program staff to identify which advocates might be a good fit for particular advocate opportunities around NCI. OAR and NCI program staff also use information to contact advocates.

Describe the secondary uses for which the PII will be used.

PII is also used to contact advocates about NCI initiatives that might be of interest to them.

Identify legal authorities governing information use and disclosure specific to the system and program.

Special Authorities of the Director – 42 U.S. Code 285a–2 authorizes the collection of the information. The information request falls under the National Cancer Institute (NCI), Office of the Director, Office of Advocacy Relations (OAR).

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

09-25-0156 Records of Participants in Programs and Respondents in Surveys Used to Evaluate

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OD

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

OMB No: 0925-0200 Expiration Date: 3/31/2027

OMB No: 0925-0774 Expiration Date: 10/31/2027

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Advocates are sent a link (via email) inviting them to join OAR's network and complete an online profile.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Advocates are not required to be a part of OAR's network. If they do not want to be a part, they can email us. We provide them the option of either having their profile categorized as inactive and save their information if they decide to re-join at a later date, or we can manually remove their information.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

If individuals need to change unexpectedly we will email users informing them of the change and allowing time for them to update their profiles to add and/or remove any information they would like to.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

If an individual expresses concern over how their information was obtained, used, or disclosed, OAR will first bring any expressed concerns to the attention of the Privacy Coordinator at the NIH Office of Management and NCI Privacy Officials. Then, OAR will discuss the incident with the individual and bring appropriate staff to discussion. OAR will work with individual, as well as any appropriate internal staff, to investigate and resolve any concern.

If an individual expresses concern over the accuracy of their information, OAR will work with them to make any updates or changes so that their record is accurate.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

There is no formal process for periodic reviews by RAS staff. However, individuals are able to update their profiles themselves to keep their PII up to date and current.

Identify who will have access to the PII in the system and the reason why they require access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Determinations are made based on Role based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Determinations are made based on Role based access controls and least privilege. User rights are provisioned based on controls within the system, allowing users only access to the minimum amount of PII necessary to perform their job.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

All staff will be trained before access is provided to them.

The NIH Security Awareness Training course is used to satisfy this requirement. According to NIH policy, all personnel who use NIH applications must attend security awareness training every year. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Response). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

Describe training system users receive (above and beyond general security and privacy awareness training).

Staff are walked though the information collected and appropriate/inappropriate uses for that information.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

General Records Schedule 08-219, Personally identifiable information extracts.

System-generated or hard copy print-outs generated for business purposes that contain Personally Identifiable Information.

Destroy when 90 days old or no longer needed pursuant to supervisory authorization, whichever is appropriate. Disposition Authority: DAA-GRS-2013-0007-0012

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

Administrative Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report.

Technical Controls:

Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data. There are technical controls in place to minimize the possibility of unauthorized access, use, and dissemination of the data in the system by requiring a user ID and password for access. The server hardware that supports this application is secured with the same controls as all other apps hosted. The actual system itself has no physical controls.

Physical Controls:

The servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.