US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/03/2024

OPDIV:

NIH

Name:

NIAID Public Intramural Research Program (IRP) Developed (PID) Authorization Boundary

PIA Unique Identifier:

P-6158261-596538

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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?

Yes

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

The National Institute of Allergies and Infectious Diseases (NIAID) Public Intramural Research Program (IRP) Developed (PID) authorization boundary consists of the following application:

Comprehensive Analysis of Ribonucleic Acid Interference (RNAi) Data (CARD)

CARD is a comprehensive web-application for integrated analysis and interactive visualization of RNAi screening data. CARD combines both existing and novel algorithms for data pre-processing, reducing false positive hits through gene expression and off-target filtering, implementing network/pathway enrichment of high-confidence hits and predicting active microRNAs (miRNA).

CARD is hosted on the Monarch Docker Platform as a Service (PaaS), which is owned and maintained by the Operations and Engineering Branch (OEB).

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

CARD: RNAi screening research data.

PII from the general public is used for registration and login, which collects name (first and last), organization/institute, email address. The end user creates their own password. Internet protocol (IP) address is collected and retained for system access records and web measurement purposes. Application logs are retained in the database.

CARD Operations and Maintenance personnel 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.

The National Institute of Allergies and Infectious Diseases (NIAID) Public Intramural Research Program (IRP) Developed (PID) authorization boundary consists of the following application:

Comprehensive Analysis of Ribonucleic Acid Interference (RNAi) Data (CARD)

CARD is a comprehensive web-application for integrated analysis and interactive visualization of RNAi screening data. CARD combines both existing and novel algorithms for data pre-processing, reducing false positive hits through gene expression and off-target filtering, implementing network/pathway enrichment of high-confidence hits and predicting active microRNAs (miRNA).

CARD is hosted on the Monarch Docker Platform as a Service (PaaS), which is owned and maintained by the Operations and Engineering Branch (OEB).

CARD: RNAi screening research data.

PII from the general public is used for registration and login, which collects name (first and last), organization/institute, email address. The end user creates their own password. Internet protocol (IP) address is collected and retained for system access records and web measurement purposes. Application logs are retained in the database.

CARD Operations and Maintenance personnel 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
Organization/institute
IP Address
Password

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

Employees
Public Citizens

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

Account creation

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

System access records and web measurement

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

42 U.S.C. 241, Research and Investigation;
42 U.S.C. 285f, National Institute on Allergy and Infectious Diseases

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Government Sources
Within the OPDIV
Non-Government Sources
Public

Identify the OMB information collection approval number and expiration date

N/A. NIH research activities are exempt from an OMB Information Collection Number through Public Law 114-255 - 21st Century Cures Act, Section 2035: Exemption for the National Institutes of Health from the Paperwork Reduction Act requirements.

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.

The user is prompted to enter the PII on the various data entry screens. For the collection of IP addresses, links to the NIH Web Policies and Notices site are available, which includes usage of Google Analytics (https://www.nih.gov/web-policies-notices).

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.

There is no process to opt out for the collection or use. Users are free to navigate to the site, but an account is required to obtain access to the application features.

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

No process required to obtain consent. There are no disclosures or any intent to expand usage of PII beyond that which is currently collected or used: user accounts and performance metrics.

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.

PII for registering for an account is self-asserted by the individual. If the user needs to update, they can create a new account. In the event that a user needs to remove their account, they may submit a request to the project administrators.

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

No process is required as there is no need validate or revalidate self-asserted information.

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.

Access to PII is assigned to personnel based upon current job responsibilities. An NIH IAM Systems account login is required to gain access to the stored PII data.

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.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). 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).

Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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.

Records are maintained throughout the life of the system in accordance with the following NIH Record Schedule:

01-003, Records of All Other Intramural Research Projects (DAA-0443-2012-0007-0003). Cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer. Destroy 7 years after cutoff.

07-203, System access records. Systems not requiring special accountability for access (DAA-GRS-2013-0006-0001). Destroy when business use ceases.

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

Administrative: Controls include performing background checks, completing training security and privacy training, and implementing role-based access for authorized users.

Technical: Active NIH account, personal identity verification (PIV) card, must be on the NIH network, passwords and secure shell (ssh) key exchange for access to system components. Encryption, intrusion prevention systems (IPSs), and intrusion detection systems (IDSs) services are provided by NIH and the Operations Engineering Branch (OEB).

Physical Controls: The physical safeguards are inherited from Amazon Web Services (AWS) which houses the system in a Federal Risk and Authorization Management Program (FedRAMP) certified facility.

Identify the publicly-available URL:

https://card.niaid.nih.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

No

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Other technologies that collect PII:

Google Analytics

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null