US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/06/2025

OPDIV:

NIH

Name:

CIT Services and Applications: Intramural Research Program (IRP) Collaborative Research Systems

PIA Unique Identifier:

P-3380288-460323

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?

Yes

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.

The Center for Information Technology (CIT) Intramural Research Program (IRP) Collaborative Research Systems collaborates with the NIH Institutes and Centers (ICs) intramural research program to provide expertise and develop software on computational research problems of significance to the ICs. IRP Collaborative Technologies provides a collection of technologies used to develop programs, queries and other software tools that are used in computational medical research. IRP Collaborative Research Services host application areas that include molecular modeling, protein structure prediction, biomedical imaging, mathematical modeling, and biomedical informatics. These may include development and pre-production versions.

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

IRP Collaborative Research Services develops tools for principal investigators to use in collecting and/or processing data. IRP Collaborative Research Services keeps a copy of the data, which depends on the research protocol, but may include personally identifiable information (PII) such as name, date of birth, phone number, photographic identifiers, medical records, medical notes, and sex. The protocol's principal investigator determine which data will be collected. All data are provided voluntarily.

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), which maintains its own unique PIA) on record, including all legal authorities documented. The purpose of the IMS 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 IMS collects unique user names and passwords (user credentials) and stores them in an encrypted format. The IMS is 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.

IRP Collaborative Research Systems is a collection of technologies used to develop programs, queries and other software tools that are used in computational medical research. The system is not used to directly collect or share data, however, it may maintain a copy of selected data depending on the medical research protocol. This data may include:
Molecular modeling
Biomedical imaging
Protein structure prediction
Mathematical modeling
Medical and bioinformatics
Research participant name
Research participant date of birth
Research participant phone number
Research participant medical records
Research participant medical notes
Research participant sex

Those requiring access to this system log in using the NIH Identity, Credential, and Access Management Services: Identity Management Services (IMS), which maintains its own unique PIA) on record, including all legal authorities documented.

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

Yes

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

Date of Birth
Name
Photographic Identifiers
Phone Numbers
Medical Records Number
Medical Notes
sex, biomedical imaging, scientific data

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

Public Citizens
Patients
No

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The PII is primarily used for medical research.

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

N/A

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

Section 301 of the Public Health Service Act, describing the general powers and duties of the Public Health Service relating to research and investigation (42 U.S.C. 241).

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.

09-25-0200; Clinical, Basic and Population-based Research Studies of the National Institutes of

Identify the sources of PII in the system.

Government Sources
Within OpDiv

Identify the OMB information collection approval number and expiration date

Public Law 114-255, section 2035 exempts 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.

Notifications are conducted by the IC or principal investigator at the time the research participant is recruited in to the study and in accordance with NIH and Intramural Research Program policies.

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.

The opt-out procedures are determined by the IC or principal investigator in accordance with NIH, Intramural Research Program, and research protocol policies. All required consent forms and notifications are handled by the IC or principal investigator at the time when the participant is recruited for the research.

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

This is not applicable because the IRP Collaborative Research Systems is not the source system

and the system does not directly collect the information from research participants. All required consent forms and notifications are handled by the IC or principal investigator at the time when the participant is recruited for the research.

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.

This is not applicable because the IRP Collaborative Research Systems is not the source system and the system does not directly collect the information from research participants. All required consent forms and notifications are handled by the IC or principal investigator at the time when the participant is recruited for the research.

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

Periodic reviews are handled in accordance with the IC policies and the research protocols. In most cases, a review is required annually in accordance with NIH Intramural Research Program policies.

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.

Administrative staff is restricted to the specific IC or principal investigator staff only. A two-factor authentication will be used. All administrative staff will sign and comply with the system administrator rules of behavior to ensure HHS and NIH operational policies are followed regarding administrator privileges and technical-use for systems/applications.

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.

When PII is accessed it is minimal information needed in accordance with HHS, NIH, and IC Least Privilege policies. This means when users have access to PII, it will be only minimally sensitive, the least PII needed, and will be used only accordance with HHS, NIH, and IC PII policy. All administrative staff will sign and comply with the system administrator rules of behavior to ensure HHS, NIH and IC operational policies are followed regarding administrator privileges and technical-use for systems/applications

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 NIH employees and direct contractors must take the NIH Information Security Awareness Course and NIH Privacy Awareness Course prior to being granted access to NIH information resources. In addition, the Information Security and Privacy Awareness Refresher must be taken annually. Administrators and Privileged Users/Developers require additional security and privacy training specific to their roles and responsibilities.

As part of the project training, employees and direct contractors are made aware of these regulations and trained in these policies.

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

Per HHS policy, personnel are exposed to security awareness materials, at least annually and prior to the employee's or direct contractor's use of, or access to, information systems through online PowerPoint presentations and/or hard-copy training. In addition, project team members will also be trained on the features and functionalities of applicable systems/applications. The frequency of this training will be initially at the start of project on-boarding, one-on-one in person training as well as online training on an as-needed basis.

Users requesting remote access are required to take specialized training courses to include Securing Remote Computers and complete a Remote Access User Certification Agreement

Users requesting Administrative rights to their assigned computers are required to complete Federal Desktop Core Configuration (FDCC) Systems Administrator Training.

There are also role-based training requirements for staff designated as having "Significant IT Security Responsibilities." These include HHS role-based training courses for Executives, Managers, and IT Administrators.

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 retained and disposed of under the authority of the NIH Records Schedule Item I-0006: Clinical Care Services Records (DAA-0443-2012-0007-0006). The Disposition: TEMPORARY. Cut off annually at end of fiscal year. Destroy 7 years after cutoff.

Item I-0007: Radiology and Imaging Records
(DAA-0443-2012-0007-0007). The Disposition: TEMPORARY. Cut off in 5 year intervals by fiscal year after file becomes inactive or when no longer needed for clinical reference, whichever is longer. Destroy 60 years after cutoff.

Item I-0010: Patient Medical Records
(DAA-0443-2012-0007-0010)
The disposition: TEMPORARY. Cut off patient case file annually after 5 years of inactivity. Destroy when case file is no longer needed for scientific reference.

Item I-0011: Medical Staff Credentialing Records
(DAA-0443-2012-0007-0011)
The disposition: TEMPORARY. Cut off annually after medical staff member leaves patient care. Transfer to inactive storage 1 year after cutoff. Destroy 30 years after cutoff.

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

The information is secured in accordance with a system classified as Federal Information Security Management Act (FISMA) Moderate" according to Federal Information Processing Standards (FIPS) 199. The security controls are specified in an up-to-date security plan. This plan restricts access and disclosure to persons as authorized in the statute, provides administrative, physical, and technical system controls, requires monitored access and promotes security training. All personnel with access to the system are required to abide by the HHS and NIH Rules of Behavior and take a non-disclosure oath upon completing security awareness training as a new hire and then annually.

Administrative controls - Management oversight of activities, security awareness and training for users of the system, conduct disaster recovery exercises, separation of duties for personnel administering the system, isolating development test instances of the system.

Technical controls - User authentication (login) and logical access controls, anti-virus software, fire walls, role based access through application. The database is behind a fire wall, with no direct access to it from outside the network.

Physical controls - Server housed in secure facility, climate control, fire alarm, fire extinguishers and Uninterrupted Power Supply (UPS) for servers.

Identify the publicly-available URL:

https://irp.nih.gov/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

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.

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?

Yes

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

Yes