US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/07/2025

OPDIV:

NIH

Name:

Office of Human Subjects Research Protections - Cloud

PIA Unique Identifier:

P-3789805-039294

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?

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 Office of Human Subjects Research Protections (OHSRP) uses the OHSRP-Cloud system to provide support to the OHSRP office and its customers for the day-to-day business functions of the OHRSP. It is used to support the internal requests for service from the OHSRP help desk. The OHSRP help desk addresses requests for service from end users relating to OHSRP program activities. The system is also used as the primary website for the NIH Institutional Review Board (IRB). Disseminating information to the users in the intramural research program but is also available to general public.

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

This system is a collection of modules consisting of commercial off the shelf (COTS) products that are hosted in the FedRAMP certified cloud service provider, Contegix Inc. The system collects the following personally identifiable information (PII): Name, Email address, Username; HHS Badge Number, Academic Degree, and training records (Collaborative Institutional Training Initiative (CITI)).

The modules of the system consist of the following modules:

JIRA (not an acronym) help desk – used to support the internal requests for service from the OHSRP help desk. The OHSRP help desk addresses requests for service from end users relating to OHSRP program activities. Information collected, maintained and stored includes program data, technical details, requests for enhancement, and general troubleshooting details.

The Office of Institutional Review Board Operations (OIRBO) confluence website – is the primary website for the IRB operations at NIH. This site is used to disseminate information to the users in the intramural research program but is also available to general public. This module will not collect data. This module disseminates information to the public that the NIH deems suitable for public distribution. No PII data is disseminated.

Users log in to the applications 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 Office of Human Subjects Research Protections (OHSRP) uses the OHSRP-Cloud system to provide support to the OHSRP office and its customers for the day-to-day business functions of the OHRSP. It is used to support the internal requests for service from the OHSRP help desk. The OHSRP help desk addresses requests for service from end users relating to OHSRP program activities. The system is also used as the primary website for the NIH Institutional Review Board (IRB). Disseminating information to the users in the intramural research program but is also available to general public.

This system is a collection of modules consisting of commercial off the shelf (COTS) products that are hosted in the FedRAMP certified cloud service provider, Contegix Inc. The system collects the following personally identifiable information (PII): Name, Email address, Username; HHS Badge Number, Academic Degree, and training records (Collaborative Institutional Training Initiative (CITI)).

The modules of the system consist of the following modules:

JIRA (not an acronym) help desk – used to support the internal requests for service from the OHSRP help desk. The OHSRP help desk addresses requests for service from end users relating to OHSRP program activities. Information collected, maintained and stored includes program data, technical details, requests for enhancement, and general troubleshooting details.

The Office of Institutional Review Board Operations (OIRBO) confluence website – is the primary website for the IRB operations at NIH. This site is used to disseminate information to the users in the intramural research program but is also available to general public. This module will not collect data. This module disseminates information to the public that the NIH deems suitable for public distribution. No PII data is disseminated.

Users log in to the applications 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
user name
HHS Badge Number
Academic Degree
training records (CITI)

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

Employees
Public Citizens
Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The PII is used to identify the OHSRP-Cloud application users, relationships to research studies, and associated actions with users such as processing, reviewing, approving and/or auditing.

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

The PII may also be used for ensuring training compliance with name and email address being used for verification against NIH IRB records.

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

42 U.S.C. §§ 241, 248, 282, 284 and 289a

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.

Published - 09-25-0216: Administration: NIH Electronic Directory

Published - 09-25-0108: Personnel: Guest Researchers, Special Volunteers, and Scientists Emeriti.

Published - SORN 09-25-0200, Clinical, Basic and Population-based Research Studies of the

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Email
Online
Government Sources
Within OpDiv
Other HHS OpDiv
Non-Governmental Sources

Identify the OMB information collection approval number and expiration date

Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements.

Public

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.

NIH staff are notified via a Privacy Act Statement that their personal information will be collected when accessing JIRA help desk's customer portal page.

Link to NIH Privacy Policy: https://www.nih.gov/privacy-policy is present on every page of our application as well, all authentication to the system and applications are all authenticated through IAM which advertises the NIH Privacy Policy as well.

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.

Users of the OHSRP voluntarily provide their PII as a condition for establishing a user account. Users may opt-out of the collection of their PII. However, refusal to provide the requested information will result in the inability to access the OHSRP system.

For researchers who are not users of the system, the NIH Principal Investigator is responsible for informing their research team members that their PII is being collected.

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

System administrators will email individuals when major changes occur to the system that are deemed to necessitate notification and consent from those individuals whose PII is in the system.

For researchers who are not users of the system, the NIH Principal Investigator is responsible for informing their research team members when major changes occur to the system.

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.

Users of the system are informed to contact the NIH IRB Office and/or their NIH Institute and Center Specific Privacy Coordinator should they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

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

The NIH IT Privacy Program requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks and interconnected systems. In addition, periodic integrity audits are conducted by system administrators and IRB Staff to ensure data integrity, availability, accuracy, relevancy, and access level.

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.

The system use a role-based access control model. Privileges are granted in accordance with least privilege: all users of the system are granted only the access required to support their job function.

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 determined by the roles granted to the user's account which is based on the user's current responsibilities in the 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.

According to NIH policy, all personnel who manage or operate NIH applications must successfully complete annual security awareness training. 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).

Users may request training on select features of the system.

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 following NIH Records Retention Schedule: Item 01-001. Records of Intramural Research Projects of Historical Significance. Intramural research records relate to planning, development, oversight and execution of biomedical research projects and programs performed by NIH research staff, contractors or under collaborative research and development agreements (CRADAs). These records span the project life cycle Disposition: Cut off annually at termination of project/program or when no longer needed for scientific reference. Transfer to the National Archives in five-year blocks when the newest records in the block are 15 years old. DAA- 0443-2012-0007-0001

Item 01-003. Records of All Other Intramural Research Projects.These intramural research records relate to planning, development, oversight and execution of biomedical research projects and programs performed by NIH research staff, contractors or under collaborative research and development agreements (CRADAs). These records span the project life cycle Disposition: Cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer. Destroy 7 years after cutoff. DAA-0443-2012-0007-0003

Item 01-005. Institutional Review Board (IRB) Records. These records document ethical and regulatory oversight of research involving human subjects as required by 45 CFR 46 and 21 CFR 56. These records document IRB activities and may include IRB procedures, membership rosters, meeting minutes, decisions/approvals, copies of reviewed research proposals, scientific evaluations, approved sample consent documents, progress reports submitted by research staff, and reports of injuries to research subjects. These records span the project life cycle. Disposition: Cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer. Destroy 7 years after cutoff. DAA-0443-2012-0007-0005.

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

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Physical Controls: The information technology (IT) hardware used to host protected information is located in a secured data center facility. The facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Identify the publicly-available URL:

irbo.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?

No

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

null