US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/05/2024

OPDIV:

NIH

Name:

NIH Research and Training Opportunities

PIA Unique Identifier:

P-1118564-913650

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

Significant System Management Change

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

The Research and Training Opportunities System (RTO) requires Multi-Factor Authentication for Users (general public).

RTO has a new configuration of the software - one database for all applications rather than separate databases for each application.

Describe the purpose of the system.

The Office of Intramural Training & Education (OITE) administers programs and initiatives to recruit and develop individuals who participate in research training activities on the NIH's main campus in Bethesda, Maryland, as well as other NIH facilities around the country. To facilitate its recruitment function, the OITE maintains the NIH Research and Training Opportunities (RTO) system, https: // www2.training.nih.gov/xfer/nihac, which includes applications and related forms for intramural

research training programs, including the Summer Internship Program (SIP), the Postbaccalaureate Training Program (PBT), the Graduate Partnerships Program (GPP), and the Undergraduate Scholarship Program (UGSP). The application system includes a back-end database that functions as a centralized repository of information regarding program applicants.

The RTO system also includes the Fellows Award for Research Excellence (FARE) application, which is unique in that it is aimed, not at prospective trainees, but at current NIH trainees who wish to participate in the annual FARE travel award competition. FARE is designed to foster and reward scientific excellence in the NIH Intramural Research Program (IRP).

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

The Research Training Opportunities (RTO) system collects information, including Personally Identifiable Information (PII), necessary (1) to evaluate the qualifications of individuals who seek intramural research training opportunities at the NIH, and (2) to contact these individuals to discuss possible training opportunities.

The RTO application system collects the following types of information: Applicant's name, email address, permanent and current address, telephone numbers, citizenship status, relative at NIH (Y/N), relative's name and Institute-Center, academic information (institutional affiliations, coursework and grades, enrollment status, grade point average, academic major, degrees earned, dates of attendance), publications, resume/curriculum vitae, cover letter/personal statement, scientific research interests, contact information for up to 3 references, letters of recommendation and evaluation ratings (submitted online by the references), eligibility information, admission preferences, standardized examination scores, reference information, mentor contact information, and dissertation research description.

The Fellows Award for Research Excellence (FARE) application collects contact information for the applicant and his/her mentor, fellowship information, an abstract of the applicant's current NIH research, and optional gender information. Abstracts sometimes contain sensitive information, including unpublished data, or novel experimental approaches.

NIH users log into the 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.

For individuals external to NIH, such as business partners, collaborators, and researchers; the system uses NIH Federated Services, a centralized authentication hub for web-based applications at NIH, instead of storing a user’s login credentials. NIH Federated login enables users to use a single authentication method via an individual’s parent organization. After the system owner approves access to an individual and registers their parent organization’s identity provider, individuals are redirected to their parent organization’s identity provider for credentials.

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

The Office of Intramural Training & Education (OITE) administers programs and initiatives to recruit and develop individuals who participate in research training activities on the NIH's main campus in Bethesda, Maryland, as well as other NIH facilities around the country. To facilitate its recruitment function, the OITE maintains the NIH Research and Training Opportunities (RTO) system, https: // www2.training.nih.gov/xfer/nihac, which includes applications and related forms for intramural

research training programs, including the Summer Internship Program (SIP), the Postbaccalaureate Training Program (PBT), the Graduate Partnerships Program (GPP), and the Undergraduate Scholarship Program (UGSP). The application system includes a back-end database that functions as a centralized repository of information regarding program applicants.

The RTO system also includes the Fellows Award for Research Excellence (FARE) application, which is unique in that it is aimed, not at prospective trainees, but at current NIH trainees who wish to participate in the annual FARE travel award competition. FARE is designed to foster and reward scientific excellence in the NIH Intramural Research Program (IRP).

The Research Training Opportunities (RTO) system collects information, including Personally Identifiable Information (PII), necessary (1) to evaluate the qualifications of individuals who seek intramural research training opportunities at the NIH, and (2) to contact these individuals to discuss possible training opportunities.

The RTO application system collects the following types of information: Applicant's name, email address, permanent and current address, telephone numbers, citizenship status, relative at NIH (Y/N), relative's name and Institute-Center, academic information (institutional affiliations, coursework and grades, enrollment status, grade point average, academic major, degrees earned, dates of attendance), publications, resume/curriculum vitae, cover letter/personal statement, scientific research interests, contact information for up to 3 references, letters of recommendation and evaluation ratings (submitted online by the references), eligibility information, admission preferences, standardized examination scores, reference information, mentor contact information, and dissertation research description.

The Fellows Award for Research Excellence (FARE) application collects contact information for the applicant and his/her mentor, fellowship information, an abstract of the applicant's current NIH research, and optional gender information. Abstracts sometimes contain sensitive information, including unpublished data, or novel experimental approaches.

NIH users log into the 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.

For individuals external to NIH, such as business partners, collaborators, and researchers; the system uses NIH Federated Services, a centralized authentication hub for web-based applications at NIH, instead of storing a user’s login credentials. NIH Federated login enables users to use a single authentication method via an individual’s parent organization. After the system owner approves access to an individual and registers their parent organization’s identity provider, individuals are redirected to their parent organization’s identity provider for credentials.

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

Yes

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

y/n - age 18 by June 15 of the current year

y/n - age 17 by June 15 of current year

optional gender information (FARE)

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

NIH trainees; NIH fellows

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary use of this information is to evaluate applicants' qualifications for research training at the NIH, including periodic updates to their record status.

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

OITE sometimes uses the email addresses provided by applicants to send them notices regarding training opportunities of potential interest to them.

Other secondary uses for system PII include:
(a) Preparing appointment paperwork;
(b) Investigating possible cases of inappropriate use of the system (e.g., violations of the NIH nepotism policy);
(c) Verifying the identity of users who contact us offline (e.g., by telephone) to report technical problems involving the system;
(d) Administering the annual FARE competition.

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

The legal authority granted to NIH to train future biomedical scientists comes from several sources. Title 42 of the U.S. Code, Sections 241 and 282(b)(13) authorize the Director, NIH, to conduct and support research training for which fellowship support is not provided under Part 487 of the Public Health Service (PHS) Act (i.e., National Research Service Awards), and that is not residency training of physicians or other health professionals. Sections 405(b)(1)(C) of the PHS Act and 42 U.S.C. Sections 284(b)(1)(C) and 285-287 grant this same authority to the Director of each of the Institutes/Centers at NIH.

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.

09-25-0158 - Administration Records of Applicants and Awardees of the Intramural Research

09-25-0014 - Clinical Research: Student Records

OPM/GOVT-1 - General Personnel Records

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

0925-0299, expiration May 2024
Renewal Started November 2023 (60-day Federal Register published)

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

Each GPP institutional and Individual Partnership has its own Memorandum of Understanding (MOU) between the NIH and the university partner. The MOUs vary in content, training duration, and financial support arrangements. MOUs are finalized by the NIH OITE and managed by key NIH personnel.

Describe the procedures for accounting for disclosures.

The OITE confers with the key NIH administrators when information about a trainee/fellow needs to be shared outside the agency.

Disclosures from RTO are unlikely to be made; however, if Privacy Act records are disclosed, the disclosing office will maintain an accounting, and the disclosures will be made in accordance with the applicable SORN.

The procedures by which GPP administrators share information with university partners and account for these disclosures vary from program to program.

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

Each collection form used by the OITE has a Privacy Act Statement notifying individuals that their PII is collected.

Inclusion of the text and/or links ensures those completing the form are well informed prior to entering data voluntarily.

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 way for prospective applicants to opt out of the collection or use of their PII. The applications and other forms collect information (including PII) that is needed to evaluate the qualifications of the individual seeking intramural research training opportunities at the NIH.

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

The OITE will confer with NIH administrators and general counsel prior to making changes in how PII is used. If there is a modification from the original intent, then a mail-merge message to each affected individual will be sent from the OITE's email address.

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.

The RTO system relies extensively on system-generated email messages, and applicants and references can contact OITE by replying to these messages. A link to OITE's "Contact Us" page, https://www.training.nih.gov/contact, is in the page footer of every RTO form. Individuals who have concerns about their PII may use the contact information on "Contact Us" page to notify RTO staff of their concerns.

The OITE will confer with key offices, including but not limited to NIH administrators, legal counsel, and ethics office, to ensure the concerns of the individual are addressed in a timely manner.

The RTO system also includes a transaction auditing module to track record changes and system activity. This module can be used by RTO administrators to investigate/confirm inappropriate or suspicious activity.

RTO system administrators have tools enabling them to modify system data (e.g., login credentials) when a breach is suspected and to disable/lock individual RTO users' accounts in cases where it is determined that the user has accessed, used, or disclosed applicant data inappropriately. In such cases, OITE disables and locks the account immediately and notifies the user, as well as his/her Information Systems Security Officer (ISS) or Scientific Director (SD), who determines the appropriate next steps.

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

RTO data are managed in accordance with the Federal record retention and disposal guidelines. Typically, an application remains in the system for one year, after which time it is archived. Archiving procedures vary from program to program; for some, archiving occurs once monthly, while for others, archiving is handled manually by system administrators. Archived applications cannot be accessed by internal RTO users, except for system developers and authorized OITE staff. Archived applications are generally retained for two years after being archived (i.e., for three years total).

System developers monitor the database and online application processes as a routine matter to ensure the data's integrity and availability.

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.

The only RTO users who can create new RTO accounts are Program Coordinators and SuperAdmins. Decisions regarding who at an Institute/Center (IC) may have access to RTO are (within limits established by OITE) left up to the Program Coordinator(s) at that IC. Occasionally

OITE will create the account after verifying from someone appropriately placed at the IC that the individual requesting access has a legitimate business need to access system data.

Program Coordinators can create view-only "Investigator" accounts; SuperAdmins can create any kind of account. As a rule, OITE will give a user elevated access within the system only when the user needs that access to do his/her job.
By default, an Investigator account gives one read-only access to the SIP and Postbac Intramural Research Training Award application pools. In cases where it is known that a user does not require access to both subsystems, a SuperAdmin can remove the user's access to one, or even both, subsystems. A SuperAdmin might remove a user's access to both subsystems if the user has agreed to serve as a mentor to an incoming summer intern and does not require access to the entire SIP applicant database. Authorized users can share individual applications with another authorized user. In these cases, the user's access to the shared applications expires after 60 days.

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 technolgoy (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).

Each RTO user has access to a role-specific RTO User's Guide. While the guides are primarily focused on how to use the system tools, some touch on such RTO policies as who may access the system, etc.

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 in RTO in accordance with the following NIH Records Schedules:

2.1.051 – Job Vacancy Case Files – Destroy 2 years after termination of register – DAA-GRS-2014-0002-0007

2.1.090 – Interview Records – Destroy 2 years after case is closed by hire or non-selection, expiration of right to appeal a non-selection, or final settlement of any associated litigation, whichever is later. – DAA-GRS-2014-0002-0008

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

Administrative Controls: RTO applies role-based security to ensure access is restricted to the appropriate user groups. All system users are required to accept the RTO Terms of Use every time they sign in. The Terms of Use page notes that the system contains information that is subject to the Privacy Act; describes the user's responsibilities regarding the safeguarding of system data; and states that unauthorized access or use of this system may subject violators to criminal, civil, and/or administrative action. At any time, Program Coordinators can disable accounts of individuals at their respective IC who leave the NIH or transfer to another IC. In addition, RTO administrators conduct a comprehensive review of all system accounts once annually, disabling/locking those belonging to individuals who are no longer at the NIH and purging all dormant accounts. Also, RTO administrators

conduct periodic and ongoing monitoring of system audits and system email traffic to identify cases of inappropriate access to or use of the system.

Technical Controls: Access to the system is controlled by NIH Login, which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, and organizational unit.

Physical Controls: The servers reside in the Office of Information Technology (OIT) hosting facility, 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.

Identify the publicly-available URL:

https://www2.training.nih.gov/xfer/nihac

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