US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/05/2024

OPDIV:

NIH

Name:

Research Training Programs Web Site

PIA Unique Identifier:

P-8646487-112495

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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.

Contractor

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.

There have been no substantive changes to the system since the last Privacy Impact Assessment (PIA) was submitted.

Describe the purpose of the system.

The purpose of the NIH Research Training Programs (RTP) website, https://www.training.nih.gov, is to provide access to the training opportunities and support services provided by NIH.

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

Account information: User's name, user credentials (email address and password), phone numbers, mailing address (Campus and Institute/Center), education records, NIH Enterprise Directory (NED) ID, and employment status.

NIH administrators 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.

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

The purpose of the NIH Research Training Programs (RTP) website, https://www.training.nih.gov, is to provide access to the training opportunities and support services provided by NIH.

Account information: User's name, email address, password, phone numbers, mailing address (Campus and Institute/Center), education records, NIH Enterprise Directory (NED) ID, and employment status.

NIH administrators 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.

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
Education Records
Employment Status
NED ID
User Credentials

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

Employees
Public Citizens
Vendor/Suppliers/Contractors
NIH trainees; NIH fellows

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

To administer Office of Intramural Training and Education (OITE) events and services, limiting access to restricted resources (e.g., NIH-only events, appointments with OITE career counselors), as appropriate.

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

Track where the NIH Intramural Research Program trainees go once they leave the NIH;

Provide networking opportunities for current trainees, NIH staff, and program alumni;

Identify individuals who are willing to serve as event speakers or contacts for OITE staff organizing training events;

Collect applicant data, including letters of recommendation, to supplement information collected via OITE's online application system (RTO);

Assess the diversity of various user groups (applicants and current trainees);

Enhance the experience of program participants (e.g., by creating personalized certificates for children of NIH staff who participate in Take Your Child to Work Day events).

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.

09-25-0140 - International Activities: International Scientific Researchers in Intramural Laboratories

09-90-0020 - Suitability for Employment Records, HHS/OS/ASPER; 09-25-0014 - Clinical Research:

OPM/GOVT-1 - General Personnel Records; OPM/GOVT-5 - Recruiting, Examining, and Placement

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the DOI

Other Federal Agencies

Non-Government Sources

Public

Identify the OMB information collection approval number and expiration date

0925-0299 (Expiration Date: May 2024)

Renewal in progress

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.

There are Memorandums of Understanding between NIH and graduate universities for the Institutional Partnerships and Individual Partnerships.

Describe the procedures for accounting for disclosures.

Disclosures from RTP 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 System of Records Notice (SORN). The OITE will confer with the NIH Senior Official for Privacy and other key NIH administrators if RTP system data involving PII need to be disclosed.

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 footer of every RTP page includes a link to our Privacy Notice, which says in part:

We maintain and dispose of electronically submitted information in accordance with the Federal Records Act (44 U.S.C. Chapter 31) and records schedules of the National Archives and Records Administration. Information may be subject to disclosure in certain cases (for example, if authorized by a Privacy Act System of Records Notice).

If you apply to one of our training programs and your application becomes part of a record system designed to retrieve PII about you by personal identifier (name, e-mail address, mailing address, phone number, etc.), we will safeguard the information you provide to us in accordance with the Privacy Act of 1974, as amended (5 U.S.C. Section 552a). We prominently display a Privacy Act Notification Statement on any form which asks you to provide personally identifiable information.

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.

Submission of personal information is voluntary; however, in order to access certain information (e. g., the Alumni Database), services (e.g., making an appointment with a career counselor), and admission consideration for certain training programs, users must complete all required fields.

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

At present, there is no process in place to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of the original collection). If there were a modification from the original intent, OITE would confer with key offices, including but not limited to the NIH Senior Official for Privacy, to determine the appropriate course of action. If deemed appropriate, OITE would notify each affected individual using the email address on record.

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 RTP system relies extensively on system-generated email messages, and registered users can in many cases contact OITE by replying to these messages. Also, the page footer of every RTP page includes a link to OITE's "Contact Us" page, https://www.training.nih.gov/contact. Individuals who have concerns about their PII can use the information on this page to notify us.

The OITE will confer with key offices, including but not limited to the NIH Senior Official for Privacy, to ensure the concerns of the individual are addressed in a timely manner.

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

RTP system administrators have tools enabling them to monitor system activity when a breach is suspected and to disable/archive individual RTP users' accounts in cases where it is determined that an unauthorized person has accessed, used, or disclosed applicant data.

All system users have access to tools to manage their passwords if they suspect that someone has accessed their data through this system.

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 contractor who maintains the RTP system, Symplicity Corp., monitors the database and system processes as a routine matter to ensure the data's integrity and availability. Also, OITE system staff informally monitor this in their day-to-day use of the system tools. There is no general process in place to ensure the accuracy and relevancy of the data, as there is no feasible way to do so. That said, the system does have business rules in place that ensure the email address provided by a new user is accurate in the sense of being accessible by that individual. The system sends an account activation link to the email address provided when a new user registers for an account. The user cannot sign in until he/she activates the account.

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.

When creating and editing system staff accounts, OITE System Admins assign roles based on each individual's job duties, using the principle of least privilege. The system allows System Admins to assign multiple roles to users when necessary and appropriate, and to remove individual rights in most cases. This gives OITE the ability to control staff members' access to PII in a fine-grained way. OITE occasionally reviews system staff accounts and adds/removes roles and rights, as appropriate.

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).

N/A

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 within RTP for a time accordance with NARA record retention schedules:

2.1.060 - Job Application Packages
Destroy 1 year after date of submission
Applications

3.2.030 - System Access Records
Destroy when business use ceases
RTP Accounts - user profiles, login files, password files, audit trails, etc

3.2.031 - System Access Records
Records are maintained within RTP for a time based on the type or data
Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.
RTP Accounts - user profiles, login files, password files, audit trails, etc

3.2.041 - System Backups and Tape Library Records
Destroy when second subsequent backup is verified as successful or when no longer needed for the system restoration, whichever is later.
RTP BackUps

5.1.030 - Records of Non-Mission Related Internal Agency Committees
Destroy when business use ceases
Alumni Database, Memberships, MyOITE

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

Administrative Controls: OITE staff access system data via a password-protected Content Management System. Other users can access their own account information or other restricted resources (e.g., the Alumni Database) by providing valid system login credentials of the proper type. RTP applies role-based security to ensure access is restricted to the appropriate user groups. At any time, System Admins can manually disable accounts of individuals who have left the NIH or no longer require access to the site.

Technical Controls: Access to the system is controlled by login name and password. Access level and permissions are controlled by the system and based on user, role, and account status. The

OITE has implemented strong password requirements for OITE staff and NIH trainees (both internal and external users) to access specific sections of the website."

Physical Controls: The RTP system is hosted in the cloud, through Amazon Web Services (AWS). The contractor who maintains the RTP system, Symplicity Corp., uses Amazon Aurora for its database needs. Amazon Aurora provides multiple levels of security at the database level. These include network isolation using Amazon Virtual Private Cloud (VPC), encryption at rest using keys created and controlled through AWS Key Management Service and encryption of data in transit using Secure Sockets Layer. On an encrypted Amazon Aurora instance, data in the underlying storage is encrypted, as are the automated backups, snapshots, and replicas in the same cluster. Communications between application and database are limited to the OITE network segment and are never exposed to a public network.

Connections to the database server are made using accounts with only the access level necessary for that connection. Connections needing only read-access to data, such as users browsing postings, are made using a database account with only read access to the specific database table they'll be reading. Similarly, update connections are made through connections granted write access only to those databases and tables they need access to.

Identify the publicly-available URL:

https://www.training.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?

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 do not collect PII:

The 'awstats' open source log file analyzer to parse Apache access

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