

# Privacy Impact Assessment Form

v 1.47.4

Status 

Form Number

Form Date

Question

Answer

1 OPDIV:

2 PIA Unique Identifier:

2a Name:

3 The subject of this PIA is which of the following?

- General Support System (GSS)  
 Major Application  
 Minor Application (stand-alone)  
 Minor Application (child)  
 Electronic Information Collection  
 Unknown

3a Identify the Enterprise Performance Lifecycle Phase of the system.

3b Is this a FISMA-Reportable system?

- Yes  
 No

4 Does the system include a Website or online application available to and for the use of the general public?

- Yes  
 No

5 Identify the operator.

- Agency  
 Contractor

6 Point of Contact (POC):

POC Title

POC Name

POC Organization

POC Email

POC Phone

7 Is this a new or existing system?

- New  
 Existing

8 Does the system have Security Authorization (SA)?

- Yes  
 No

8a Date of Security Authorization

9 Indicate the following reason(s) for updating this PIA. Choose from the following options.

- PIA Validation (PIA Refresh/Annual Review)
- Anonymous to Non-Anonymous
- New Public Access
- Internal Flow or Collection
- Commercial Sources
- Significant System Management Change
- Alteration in Character of Data
- New Interagency Uses
- Conversion

10 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.

11 Describe the purpose of the system.

The Office of Intramural Training & Education (OITE) administers programs and initiatives to recruit and develop

12 Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)

The Research Training Opportunities (RTO) system collects information, including Personally Identifiable Information (PII), necessary (1) to evaluate the qualifications of individuals who

13 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

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

- Yes
- No

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

- Social Security Number
- Name
- Driver's License Number
- Mother's Maiden Name
- E-Mail Address
- Phone Numbers
- Medical Notes
- Certificates
- Education Records
- Military Status
- Foreign Activities
- Taxpayer ID
- Date of Birth
- Photographic Identifiers
- Biometric Identifiers
- Vehicle Identifiers
- Mailing Address
- Medical Records Number
- Financial Account Info
- Legal Documents
- Device Identifiers
- Employment Status
- Passport Number

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)

16	Indicate the categories of individuals about whom PII is collected, maintained or shared. <input checked="" type="checkbox"/> Employees <input checked="" type="checkbox"/> Public Citizens <input type="checkbox"/> Business Partners/Contacts (Federal, state, local agencies) <input checked="" type="checkbox"/> Vendors/Suppliers/Contractors <input type="checkbox"/> Patients Other <input type="text" value="NIH trainees; NIH fellows"/>
17	How many individuals' PII is in the system? <input type="text" value="100,000-999,999"/>
18	For what primary purpose is the PII used? <input type="text" value="The primary use of this information is to evaluate applicants' qualifications for research training at the NIH, including periodic updates to their record status."/>
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research) <input type="text" value="OITE sometimes uses the email addresses provided by applicants to send them notices regarding training opportunities of potential interest to them.&lt;br/&gt;&lt;br/&gt;Other secondary uses for system PII include:&lt;br/&gt;(a) Preparing appointment paperwork;&lt;br/&gt;(b) Investigating possible cases of inappropriate use of the system (e.g., violations of the NIH nepotism policy);&lt;br/&gt;(c) Verifying the identity of users who contact us offline (e.g., by telephone) to report technical problems involving the system;&lt;br/&gt;(d) Administering the annual FARE competition."/>
20	Describe the function of the SSN. <input type="text" value="n/a"/>
20a	Cite the <b>legal authority</b> to use the SSN. <input type="text" value="n/a"/>
21	Identify <b>legal authorities</b> governing information use and disclosure specific to the system and program. <input type="text" value="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."/>
22	Are records on the system retrieved by one or more PII data elements? <input checked="" type="radio"/> Yes <input type="radio"/> No

22a

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.

- Published: OPM/GOVT-1 - General Personnel Records  
OPM/GOVT-5 - Recruiting, Examining, and Placement Records
- Published: 09-25-0014 - Clinical Research: Student Records  
09-25-0108 - Personnel: Guest Researchers, Special Volunteers, and Scientists Emeriti
- Published: 09-25-0158 - Administration Records of Applicants and Awardees of the Intramural Research Training Awards Program

In Progress

23

Identify the sources of PII in the system.

- Directly from an individual about whom the information pertains
  - In-Person
  - Hard Copy: Mail/Fax
  - Email
  - Online
  - Other
- Government Sources
  - Within the OPDIV
  - Other HHS OPDIV
  - State/Local/Tribal
  - Foreign
  - Other Federal Entities
  - Other
- Non-Government Sources
  - Members of the Public
  - Commercial Data Broker
  - Public Media/Internet
  - Private Sector
  - Other

23a

Identify the OMB information collection approval number and expiration date.

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

24

Is the PII shared with other organizations?

- Yes
- No

24a Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

PII may be shared with NIH Investigators and administrators for admissions and appointment paperwork. Records may also be disclosed to student volunteers, individuals working under a personal services contract, and other individuals performing functions for HHS who do not technically have the status of agency employees, if they need the records in the performance of their agency functions.

Other Federal Agency/Agencies

Disclosure may be made to the Department of Justice or to a court or other tribunal when (a) HHS, or any component thereof; or (b) any HHS employee in his or her official capacity; or (c) any HHS employee in his or her individual capacity where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the employee; or (d) the United States or any agency thereof where HHS determines that the litigation is likely to affect HHS or any of its components, is a party to litigation or has an interest in such litigation, and HHS determines that the use of such records by the Department of Justice, court or other tribunal is relevant and necessary to the litigation and would help in the effective representation of the governmental party, provided, however, that in each case HHS determines that such disclosure is compatible with the purpose for which the records were collected.

State or Local Agency/Agencies

Disclosure may be made to a Federal, State or local agency maintaining civil, criminal or other pertinent records, such as current licenses, if necessary to obtain a record relevant to an agency decision concerning the selection or retention of a fellow.

Private Sector

Disclosure may be made to institutions providing financial support.

24b Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).

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.

24c Describe the procedures for accounting for disclosures	<p>The OITE confers with the key NIH administrators when information about a trainee/fellow needs to be shared outside the agency.</p> <p>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.</p> <p>The procedures by which GPP administrators share information with university partners and account for these disclosures vary from program to program.</p>	
25 Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.	<p>Each collection form used by the OITE has a Privacy Act Statement notifying individuals that their PII is collected.</p> <p>Inclusion of the text and/or links ensures those completing the form are well informed prior to entering data voluntarily.</p>	
26 Is the submission of PII by individuals voluntary or mandatory?	<p><input checked="" type="radio"/> Voluntary</p> <p><input type="radio"/> Mandatory</p>	
27 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.	<p>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.</p>	
28 Describe the process to notify and obtain consent from the 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 original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	<p>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.</p>	

29 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. If no process exists, explain why not.

The RTO system relies extensively on system-generated email messages, and applicants and references can contact OITE by replying to these messages. Also, there is a link to OITE's "Contact Us" page, <https://www.training.nih.gov/contact>, in the page footer of every RTO form. 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 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.

30 Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.

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.

<p>31 Identify who will have access to the PII in the system and the reason why they require access.</p>	<input checked="" type="checkbox"/> Users	<p>NIH personnel who are involved in the recruitment and selection of NIH trainees. These individuals require</p>
	<input checked="" type="checkbox"/> Administrators	<p>OITE personnel that have view/edit access to RTO accounts, applications, reports, and administrative tools.</p>
	<input checked="" type="checkbox"/> Developers	<p>System developers monitor the database and online application processes as a routine matter to ensure</p>
	<input checked="" type="checkbox"/> Contractors	<p>Direct contractors and NIH IT staff who are responsible for managing/maintaining all aspects of the</p>
	<input type="checkbox"/> Others	
<p>32 Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.</p>	<p>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</p>	
<p>33 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.</p>	<p>The only RTO users who can create new RTO accounts are Program Coordinators and SuperAdmins. Decisions regarding who at an 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.</p> <p>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 IRTA 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.</p>	
<p>34 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.</p>	<p>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 <a href="http://irtsectraining.nih.gov">http://irtsectraining.nih.gov</a> site with valid NIH credentials.</p>	



35 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.	
36 Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	<input checked="" type="radio"/> Yes <input type="radio"/> No	
37 Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	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	
38 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 Institutes and Centers (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.	

39 Identify the publicly-available URL:

Summer Internship Program (series of subprograms) -  
<https://www2.training.nih.gov/transfer/SIPApp>

Undergraduate Scholarship Program -  
<https://www2.training.nih.gov/transfer/UGSPApp>

Postbaccalaureate IRTA Training Program -  
<https://www2.training.nih.gov/transfer/PBTApp>

Graduate Partnerships Program -  
<https://www2.training.nih.gov/transfer/GPPApp>

Fellows Award for Research Excellence (FARE) -  
<https://www2.training.nih.gov/transfer/fareapp>

40 Does the website have a posted privacy notice?  Yes  
 No

40a Is the privacy policy available in a machine-readable format?  Yes  
 No

41 Does the website use web measurement and customization technology?  Yes  
 No

41a Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)

Technologies	Collects PII?
<input type="checkbox"/> Web beacons	<input type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/> Web bugs	<input type="radio"/> Yes <input type="radio"/> No
<input checked="" type="checkbox"/> Session Cookies	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="checkbox"/> Persistent Cookies	<input type="radio"/> Yes <input type="radio"/> No
Other... <input type="text"/>	<input type="radio"/> Yes <input type="radio"/> No

42 Does the website have any information or pages directed at children under the age of thirteen?  Yes  
 No

43 Does the website contain links to non- federal government websites external to HHS?  Yes  
 No

43a Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?  Yes  
 No

General Comments

This component is under the Office of the Director General Support System (OD GSS), whose Universal Unique Identifier (UUID) is: 2092B382-A4F2-4FD5-A93E-1857E18B771E.

OPDIV Senior Official  
for Privacy Signature

**Dustin B.  
Close -S**

Digitally signed by Dustin  
B. Close -S  
Date: 2024.01.03 10:39:30  
-05'00'

# Privacy Impact Assessment Form

v 1.47.4

Status 

Form Number

Form Date

Question

Answer

1 OPDIV:

2 PIA Unique Identifier:

2a Name:

3 The subject of this PIA is which of the following?

- General Support System (GSS)  
 Major Application  
 Minor Application (stand-alone)  
 Minor Application (child)  
 Electronic Information Collection  
 Unknown

3a Identify the Enterprise Performance Lifecycle Phase of the system.

3b Is this a FISMA-Reportable system?

- Yes  
 No

4 Does the system include a Website or online application available to and for the use of the general public?

- Yes  
 No

5 Identify the operator.

- Agency  
 Contractor

6 Point of Contact (POC):

POC Title

POC Name

POC Organization

POC Email

POC Phone

7 Is this a new or existing system?

- New  
 Existing

8 Does the system have Security Authorization (SA)?

- Yes  
 No

8a Date of Security Authorization

9 Indicate the following reason(s) for updating this PIA. Choose from the following options.

<input checked="" type="checkbox"/> PIA Validation (PIA Refresh/Annual Review)	<input type="checkbox"/> Significant System Management Change
<input type="checkbox"/> Anonymous to Non-Anonymous	<input type="checkbox"/> Alteration in Character of Data
<input type="checkbox"/> New Public Access	<input type="checkbox"/> New Interagency Uses
<input type="checkbox"/> Internal Flow or Collection	<input type="checkbox"/> Conversion
<input type="checkbox"/> Commercial Sources	

10 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.

11 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

12 Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)

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.

13 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

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

Yes  
 No

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

<input type="checkbox"/> Social Security Number	<input type="checkbox"/> Date of Birth
<input checked="" type="checkbox"/> Name	<input type="checkbox"/> Photographic Identifiers
<input type="checkbox"/> Driver's License Number	<input type="checkbox"/> Biometric Identifiers
<input type="checkbox"/> Mother's Maiden Name	<input type="checkbox"/> Vehicle Identifiers
<input checked="" type="checkbox"/> E-Mail Address	<input checked="" type="checkbox"/> Mailing Address
<input checked="" type="checkbox"/> Phone Numbers	<input type="checkbox"/> Medical Records Number
<input type="checkbox"/> Medical Notes	<input type="checkbox"/> Financial Account Info
<input type="checkbox"/> Certificates	<input type="checkbox"/> Legal Documents
<input checked="" type="checkbox"/> Education Records	<input type="checkbox"/> Device Identifiers
<input type="checkbox"/> Military Status	<input checked="" type="checkbox"/> Employment Status
<input type="checkbox"/> Foreign Activities	<input type="checkbox"/> Passport Number
<input type="checkbox"/> Taxpayer ID	

NED ID  
User Credentials

16	<p>Indicate the categories of individuals about whom PII is collected, maintained or shared.</p> <p><input checked="" type="checkbox"/> Employees  <input checked="" type="checkbox"/> Public Citizens  <input type="checkbox"/> Business Partners/Contacts (Federal, state, local agencies)  <input checked="" type="checkbox"/> Vendors/Suppliers/Contractors  <input type="checkbox"/> Patients</p> <p>Other <input type="text" value="NIH trainees; NIH fellows"/></p>
17	<p>How many individuals' PII is in the system?</p> <p><input type="text" value="50,000-99,999"/></p>
18	<p>For what primary purpose is the PII used?</p> <p><input type="text" value="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."/></p>
19	<p>Describe the secondary uses for which the PII will be used (e.g. testing, training or research)</p> <p><input type="text" value="Track where the NIH-IRP 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)."/></p>
20	<p>Describe the function of the SSN.</p> <p><input type="text" value="N/A"/></p>
20a	<p>Cite the <b>legal authority</b> to use the SSN.</p> <p><input type="text" value="N/A"/></p>
21	<p>Identify <b>legal authorities</b> governing information use and disclosure specific to the system and program.</p> <p><input type="text" value="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."/></p>
22	<p>Are records on the system retrieved by one or more PII data elements?</p> <p><input checked="" type="radio"/> Yes  <input type="radio"/> No</p>

22a

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.

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

Published: 09-90-0020 - Suitability for Employment Records, HHS/OS/ASPER; 09-25-0014 - Clinical Research: Student Records, HHS/NIH/OD/OIR/

Published: 09-25-0140 - International Activities: International Scientific Researchers in Intramural Laboratories at the National Institutes of Health,

In Progress

23

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hard Copy: Mail/Fax

Email

Online

Other

Government Sources

Within the OPDIV

Other HHS OPDIV

State/Local/Tribal

Foreign

Other Federal Entities

Other

Non-Government Sources

Members of the Public

Commercial Data Broker

Public Media/Internet

Private Sector

Other

23a

Identify the OMB information collection approval number and expiration date.

0925-0299 (Expiration Date: May 2024)  
Renewal in-progress

24

Is the PII shared with other organizations?

Yes

No

24a Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

PII may be shared with NIH Investigators and administrators for admissions and appointment paperwork. Records may also be disclosed to student volunteers, individuals working under a personal services contract, and other individuals performing functions for HHS who do not technically have the status of agency employees, if they need the records in the performance of their agency functions.

Other Federal Agency/Agencies

Disclosure may be made to the Department of Justice or to a court or other tribunal when (a) HHS, or any component thereof; or (b) any HHS employee in his or her official capacity; or (c) any HHS employee in his or her individual capacity where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the employee; or (d) the United States or any agency thereof where HHS determines that the litigation is likely to affect HHS or any of its components, is a party to litigation or has an interest in such litigation, and HHS determines that the use of such records by the Department of Justice, court or other tribunal is relevant and necessary to the litigation and would help in the effective representation of the governmental party, provided, however, that in each case HHS determines that such disclosure is compatible with the purpose for which the records were collected.

State or Local Agency/Agencies

Disclosure may be made to a Federal, State or local agency maintaining civil, criminal or other pertinent records, such as current licenses, if necessary to obtain a record relevant to an agency decision concerning the selection or retention of a fellow.

Private Sector

Disclosure may be made to institutions providing financial support. Also, responses to the "Amgen Scholars Program at NIH - Supplemental Application" survey are shared with the corporate sponsor that provides financial support for that program.

24b Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).

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



24c 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.	
25 Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.	<p>The footer of every RTP page includes a link to our Privacy Notice, which says in part:</p> <p>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).</p> <p>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.</p>	
26 Is the submission of PII by individuals voluntary or mandatory?	<p><input checked="" type="radio"/> Voluntary</p> <p><input type="radio"/> Mandatory</p>	
27 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.	
28 Describe the process to notify and obtain consent from the 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 original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	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.	

29 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. If no process exists, explain why not.

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.

30 Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.

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.

<p>31 Identify who will have access to the PII in the system and the reason why they require access.</p>	<input checked="" type="checkbox"/> Users	<p>To modify/update their profile data and change their account preferences.</p>
	<input checked="" type="checkbox"/> Administrators	<p>To (1) generate reports for program evaluation purposes; (2) ensure data integrity/accuracy/etc.; (3) maintain</p>
	<input checked="" type="checkbox"/> Developers	<p>To ensure proper functioning of the system and assist OITE with technical issues.</p>
	<input checked="" type="checkbox"/> Contractors	<p>Direct and Non-Direct contractors. To support Administrators and Developers.</p>
	<input checked="" type="checkbox"/> Others	<p>Registered NIH Trainees, NIH Staff, and Alumni have access to Alumni Database, for career networking</p>
<p>32 Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.</p>	<p>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</p>	
<p>33 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.</p>	<p>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.</p>	
<p>34 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.</p>	<p>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 <a href="http://irtsectraining.nih.gov">http://irtsectraining.nih.gov</a> site with valid NIH credentials.</p>	
<p>35 Describe training system users receive (above and beyond general security and privacy awareness training).</p>	<p>N/A</p>	
<p>36 Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?</p>	<p><input checked="" type="radio"/> Yes <input type="radio"/> No</p>	

37 Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.

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

38 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. Also, OITE is in the process of implementing strong password requirements across the site, for both internal and external users. This update will be complete by late November 2019.

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.

39 Identify the publicly-available URL:

40 Does the website have a posted privacy notice?  Yes  No

40a Is the privacy policy available in a machine-readable format?  Yes  No

41 Does the website use web measurement and customization technology?  Yes  No

41a Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)


Technologies	Collects PII?
<input type="checkbox"/> Web beacons	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="checkbox"/> Web bugs	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input checked="" type="checkbox"/> Session Cookies	<input checked="" type="radio"/> Yes <input type="radio"/> No
<input type="checkbox"/> Persistent Cookies	<input type="radio"/> Yes <input checked="" type="radio"/> No
Other... The 'awstats' open source log file analyzer to parse Apache access	<input type="radio"/> Yes <input checked="" type="radio"/> No

42 Does the website have any information or pages directed at children under the age of thirteen?  Yes  No

43 Does the website contain links to non- federal government websites external to HHS?  Yes  No

43a Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?  Yes  No

General Comments	This component is under the OD GSS, whose Universal Unique Identifier (UUID) is: 2092B382-A4F2-4FD5-A93E-1857E18B771E.
------------------	--

OPDIV Senior Official for Privacy Signature	<b>Dustin B. Close -S</b>  Digitally signed by Dustin B. Close -S Date: 2024.01.03 12:07:47 -05'00'
---	---