US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

02/25/2026

OPDIV:

NIH

Name:

OITE Content Management System

PIA Unique Identifier:

P-8891463-659798

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Development

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 Intramural Training & Education Content Management System Website (OITE CMS) enables the National Institutes of Health (NIH) to recruit and train scientists to lead the biomedical research community of the future and improve human health. The CMS website redirects users to trainings they can apply to on a separate platform. The primary purpose of the OITE CMS website is to disseminate knowledge by providing professional development and career advancement metadata and links to the end user (as opposed to collecting information from the user).

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

The OITE CMS collects and maintains the following personally identifiable information (PII):

First Name
Last Name
Work Email Address
Work Address (Campus Location)

Phone Number
User ID
Education Level/Degrees
Organization or Institute/Center
Trainee Level (examples: Postbac, Grad Student, Postdoc,…)
NIH Internship Program (examples: Graduate Partnership Program, Undergraduate Scholarship Program,…)
Job Title/Role
Badge ID

The OITE CMS website does not share any information outside of OITE. Any stored information is routinely purged in accordance with federal records management guidelines.

The type of information that is provided through the OITE CMS website is linked to the public domain and is non-sensitive. The website and related tools do this by ensuring compliance with best practices, including agile and user-centered design; federal plain language guidelines; accessibility; and effective management of web content. The system is hosted in Science and Technology Research Infrastructure for Discovery, Experimentation, and Sustainability (STRIDES) boundary. STRIDES maintains its own Privacy Impact Assessment (PIA).

Users log in to 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 Office of Intramural Training & Education Content Management System Website (OITE CMS) enables the National Institutes of Health (NIH) to recruit and train scientists to lead the biomedical research community of the future and improve human health. The CMS website redirects users to trainings they can apply to on a separate platform. The primary purpose of the OITE CMS website is to disseminate knowledge by providing professional development and career advancement metadata and links to the end user (as opposed to collecting information from the user).

The OITE CMS collects and maintains the following personally identifiable information (PII):

First Name
Last Name
Work Email Address
Work Address (Campus Location)
Phone Number
User ID
Education Level/Degrees
Organization or Institute/Center
Trainee Level (examples: Postbac, Grad Student, Postdoc,…)
NIH Internship Program (examples: Graduate Partnership Program, Undergraduate Scholarship Program,…)
Job Title/Role
Badge ID

The OITE CMS website does not share any information outside of OITE. Any stored information is routinely purged in accordance with federal records management guidelines.

The type of information that is provided through the OITE CMS website is linked to the public domain and is non-sensitive. The website and related tools do this by ensuring compliance with best practices, including agile and user-centered design; federal plain language guidelines; accessibility; and effective management of web content. The system is hosted in Science and Technology Research Infrastructure for Discovery, Experimentation, and Sustainability (STRIDES) boundary. STRIDES maintains its own Privacy Impact Assessment (PIA).

Users log in to 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
Organization or Institute/Center
Trainee Level
NIH Internship Program
Job Title/Role
Badge ID/User ID

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

Employees
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

To ensure users are able to log into the system to access the service. Users access services based on their respective education level.

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

Identify key metrics of users for the website, e.g. usability and utilization of resources.

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

42 U.S. Code § 241

42 U.S. Code § 282
42 U.S. Code § 284
42 U.S. Code § 281

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.

09-25-0014 - Clinical Research: Student Records

OPM/GOVT-1 - General Personnel Records

09-25-0158 - Administration Records of

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

Within the OMB

Identify the OMB information collection approval number and expiration date

OMB Number: 0925-0299

Expiration Date: 03/31/2027

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.

During the registration process, customers are requested to provide their consent for the collection and utilization of their name, email address, and phone number.

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.

It is important to note that while users have the option to opt out, customers must understand that without providing the required information, they will be unable to complete their registration or access the website services.

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.

If an individual has specific concerns regarding their PII usage, they may contact OITE CMS personnel through the "Contact Us" page listed here: https://www.training.nih.gov/welcome-to-the-nih-oite/contact-us/

The emails listed are as follows: OITE-private@nih.gov (For policy and personnel questions) and OITE@nih.gov (For general questions).

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

There is a data review every six months to purge any data no longer being used for reports.

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.

Authorization to system and data 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.

Authorization to system and data 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. A NIH IAM Systems account login is required to gain access to the stored PII data.

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 and privacy 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).

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 in OITE CMS in accordance with the following NIH Records Schedules:

06-601 – Non-mission employee training program records. Destroy when 3 years old, or 3 years after superseded or obsolete, whichever is appropriate, but longer retention is authorized if required for business use. DAA-GRS-2016-0014-0001

06-605 – Mission-Related Training Records. Cut off at end of the fiscal year in which the course material is superseded or becomes obsolete. Destroy 5 years after cutoff. Longer retention is authorized if required for business use. DAA-0443-2019-0005-0008

06-606 – Individual Employee Training Records. Destroy when superseded, 3 years old, or 1 year after separation, whichever comes first, but longer retention is authorized if required for business use. DAA-GRS-2016- 0014-0003

06-901 – Non-Employee Fellowship Records. Destroy 3 years after completion of fellowship, termination of agreement, or non-acceptance of application. Longer retention is authorized if required for business use. Disposition Authority Agency (DAA)-0443-2020-0002-0001

06-902 – Visiting Fellow and Visiting Fellow scientist Immigration and Work Authorization Records. Destroy 3 year(s) after completion of fellowship, termination of agreement, or non-acceptance of application. Longer retention is authorized if required for business use. Disposition Authority: DAA-0443-2020-0002-0001

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

Administrative Controls: OITE CMS applies role-based security to ensure access is restricted to the appropriate user groups. Administrators can disable accounts of individuals at their respective Institutes and Centers (IC) who leave the NIH or transfer to another IC. In addition, OITE CMS 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, OITE CMS administrators conduct periodic and ongoing monitoring of system audits and system 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 Amazon Webs Services (AWS) GovCloud (STRIDES), where AWS policies and procedures are in place to restrict access to the machines. Physical access to AWS data centers are beyond the scope of OITE CMS. Access to the virtualized AWS resources require NIH Login credentials.

Identify the publicly-available URL:

https://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?

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