

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/08/2024

OPDIV:

NIH

Name:

NIAID Collaborator Learning Management Solutions (NCLMS)

PIA Unique Identifier:

P-9607666-950545

The subject of this PIA is which of the following?

Minor Application (child)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

No

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

Yes

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.**Describe the purpose of the system.**

National Institute of Allergy and Infectious Disease (NIAID) Collaborator Learning Management Solutions (NCLMS) is a Monarch hosted Learning Management System (LMS). NCLMS offers Division of AIDS (DAIDS) clinical research staff, collaborators, and training partners the ability to complete online training courses and track training progress.

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

NCLMS is a Monarch hosted Learning Management System (LMS). NCLMS offers Division of AIDS (DAIDS) clinical research staff, collaborators, and training partners the ability to complete online training courses and track training progress.

The information types collected include: Name, email, and certificates. The primary purpose of the personally identifiable information (PII) is to retain information of specific courses passed in order to print certificates.

NIH Users log in to this system using the iTrust/NIH Login Services with organizational provided credentials, National Institutes of Health Personal Identity Verification (NIH PIV), which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of iTrust/NIH Login 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 Trust/NIH Login Services collects unique user names and passwords (user credentials) and stores them in an encrypted format. The iTrust/NIH Login Services are an essential service which facilitates and governs network access to various resources.

Non-organizational users must choose from the provided list of account authentication providers (Google, Login.gov, Microsoft, etc.) and that entity conducts the identification verification and authentication of the account entered. NCLMS does not have the ability to manage the accounts created through those entities.

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

National Institute of Allergy and Infectious Disease (NIAID) Collaborator Learning Management Solutions (NCLMS) is a Monarch hosted Learning Management System (LMS). NCLMS offers Division of AIDS (DAIDS) clinical research staff, collaborators, and training partners the ability to complete online training courses and track training progress.

The information types collected include: Name, email, and certificates. The primary purpose of the PII is to retain information of specific courses passed in order to print certificates.

NIH Users log in to this system using the iTrust/NIH Login Services with organizational provided credentials (NIH PIV) which maintains its own unique privacy impact assessment (PIA) on record, including all legal authorities documented. The purpose of iTrust/NIH Login 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 Trust/NIH Login Services collects unique user names and passwords (user credentials) and stores them in an encrypted format. The iTrust/NIH Login Services are an essential service which facilitates and governs network access to various resources.

Non-organizational users must choose from the provided list of account authentication providers (Google, Login.gov, Microsoft, etc.) and that entity conducts the identification verification and authentication of the account entered. NCLMS does not have the ability to manage the accounts created through those entities.

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
Certificates

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

Employees
Public Citizens

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The primary purpose of the PII is to retain information of specific courses passed in order to print certificates.

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

The PII is used in reporting administrative information.

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

42 U.S.C. 241

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, HHS/NIH/CC

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Identify the OMB information collection approval number and expiration date

Not applicable (N/A). As Non-Applicable (N/A). As Public Law 114-255, Section 2035, exempts research conducted by NIH

from Paperwork Reduction Act (PRA) requirements.

Private Sector

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.

PII is provided by the person choosing to take a course. If they do not provide the PII, they will not be able to take the course nor obtain the certificate showing that they completed the course successfully. This information is required when arranging to take a course and therefore no prior notice is given.

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 opt-out option. Individuals may decide to not provide their PII. However, in doing so, they will not be able to take the course.

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

Following the notification procedures within SORN 09-25-0014, Clinical Research: Student Records, HHS/NIH/CC, the mechanisms available to notify users who take training from the NCLMS whose PII may be impacted, are by posting such a notification on the home page. The banner on the

training pages states should the system be impacted (PII breach, outages, etc) the users will be notified via email address provided. A follow-up email is then sent to the users email address provided which reiterates the impact.

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.

Individuals with concern about or updates of their PII always have the ability to contact the NCLMS Help Desk, which will address their concerns or make requested changes.

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

Each person's training is a single / individual effort, therefore no periodic reviews of the PII are needed. While records of certificate completion are kept for user retrieval and tracking purposes, it is incumbent upon the user to reach out and update PII associated with their profile.

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.

Other than those taking the training courses, the only others with access are the NCLMS administrators and help desk personnel. Administrators and help desk personnel are granted access to PII in accordance with their explicit roles as they perform their administrative responsibilities.

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.

Administrators and help desk personnel are granted access to PII in accordance with their explicit roles as they perform their administrative responsibilities.

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 (employees and direct contractors) must complete the annual mandatory security, privacy and information management awareness training prior to the use of, or access to, information systems. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Emergency Preparedness and Records Management).

Describe training system users receive (above and beyond general security and privacy awareness training).

When an administrator or help desk personnel is given access to the NCLMS the Business Process Information Management Branch (BPIMB) Operations Manager ensures that the person is trained on its use, including access controls and restrictions.

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.

06-606 Individual Employee Training Records

Records documenting training required by all or most Federal agencies, such as information system security and anti-harassment training, and training to develop job skills. Records may include, completion certificates or verification documents for mandatory training required of all Federal;

employees or specific groups of employees (e.g., supervisors, contractors); Individual Development Plans (IDPs); and mentoring or coaching agreements.

Exclusion: Academic transcripts, professional licenses, civil service exams, or documentation of mission-related training are not covered by this item.

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

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

Administrative controls : Securing PII is provided through the formal process of granting permission-based access to each NCLMS for each type of user. Each end user has access to the specific LMS modules for which they have permission to access. Administrative users are granted administrative access to the NCLMS and specific LMS as determined by the BPIMB Operations Manager.

Technical Controls: Technical Safeguards include restricting access to authenticated users using secure socket layer encryption, a two-factor authentication and role-based access controls.

Physical Controls: Physical Safeguards include physical access to the system is controlled by security guards, employee badging, proximity cards, card readers, and security cameras. Access to the server is controlled by card readers at the server room door. There is a battery backup for power until the backup generator starts. Fire protection including sprinklers, and flooding sensors at the floor level.

Identify the publicly-available URL:

<https://daidslearningportal.niaid.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 under 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