US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/23/2025

OPDIV:

NIH

Name:

NIAID Laboratory Information Management Systems (LIMS)

PIA Unique Identifier:

P-4774271-111378

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?

No

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 National Institute of Allergies and Infectious Diseases (NIAID) Laboratory Information Management Systems (LIMS) authorization boundary consists of three applications:

Data Integration and Data Entry Management (DIADEM) is an internally-facing, web application that enables automated data upload from high-throughput lab instrumentation, long-term storage, cross-team data sharing, and improved data retrieval processes. This application is hosted on the NIAID Monarch cloud platform maintained by the Operations Enterprise Branch (OEB).

Flow-Cytometry Experiment and Reagent Management System (FERMS) supports the design and tracking of Flow Cytometry experiments. FERMS includes a database of flow cytometry reagents and provides knowledge-based design of protocols and experimental runs which is key to the mission of its sponsors. The sponsor has a long-term goal of increasing the degree of knowledge-based experimental design, based on accumulated experience with results obtained from specific protocol designs.

Vaccine Research Center (VRC) Humoral Immunology Core Laboratory Information Management System (VHICL-IMS)
VHICL-IMS enables end-to-end, systematic tracking and reporting of details pertaining to antibody binding and neutralization studies conducted at the Humoral Immunology Core (HIMC). VHICL-IMS allows tracking of studies, experiments, assays, and reagents and assay data.
FERMS and VHICL-IMS are hosted by OEB in the NIAID Research and Development Computing Facility.

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

The types of information collected, maintained, or shared by LIMS systems are as follows:

DIADEM - Research product development data.

FERMS - Details about the parameters of Flow Cytometry experiments, specifically what reagents were used in experiments (antibodies, flourophores) and what dates experiments were conducted.

VHICL-IMS collects, uses, and maintains research related information from humoral immunology studies, experiments, assays, reagents, and assay data.

PII within LIMS is limited to NIH personnel (current and former) work related information. Researchers perform experiment data entry, analysis, and report generation using these systems. The PII that is collected about the research personnel in these systems is to identify the persons doing the entry, analysis, and reporting and provides basic contact information about them such as their NIH email address and laboratory affiliation. Name, work email address, organization, and job title are sourced from the NIH Enterprise Directory (NED), which is managed by NIH Center for Information Technology (CIT) or the NIAID Employee Assignment Registry (NEAR), which maintains their own PIA, including all legal authorities documented.

Users log in to the systems 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 LIMS authorization boundary consists of three applications:
Data Integration and Data Entry Management (DIADEM) is an internally-facing, web application that enables automated data upload from high-throughput lab instrumentation, long-term storage, cross-team data sharing, and improved data retrieval processes. This application is hosted on the NIAID Monarch cloud platform maintained by the Operations Enterprise Branch (OEB).

Flow-Cytometry Experiment and Reagent Management System (FERMS) supports the design and tracking of Flow Cytometry experiments. FERMS includes a database of flow cytometry reagents and provides knowledge-based design of protocols and experimental runs which is key to the mission of its sponsors. The sponsor has a long-term goal of increasing the degree of knowledge-based experimental design, based on accumulated experience with results obtained from specific protocol designs.
Vaccine Research Center (VRC) Humoral Immunology Core Laboratory Information Management System (VHICL-IMS)
VHICL-IMS enables end-to-end, systematic tracking and reporting of details pertaining to antibody

binding and neutralization studies conducted at the Humoral Immunology Core (HIMC). VHICL-IMS allows tracking of studies, experiments, assays, and reagents and assay data.
FERMS and VHICL-IMS are hosted by OEB in the NIAID Research and Development Computing Facility.
The types of information collected, maintained, or shared by LIMS systems are as follows:
DIADEM - Product development data.

FERMS - Details about the parameters of Flow Cytometry experiments, specifically what reagents were used in experiments (antibodies, flourophores) and what dates experiments were conducted.

VHICL-IMS collects, uses, and maintains research related information from humoral immunology studies, experiments, assays, reagents, and assay data.

PII within LIMS is limited to NIH personnel (current and former) work related information. Researchers perform experiment data entry, analysis, and report generation using these systems. The PII that is collected about the research personnel in these systems is to identify the persons doing the entry, analysis, and reporting and provides basic contact information about them such as their NIH email address and laboratory affiliation. Name, work email address, organization, and job title are sourced from the NIH Enterprise Directory (NED), which is managed by NIH Center for Information Technology (CIT) or the NIAID Employee Assignment Registry (NEAR), which maintains their own PIA, including all legal authorities documented.

Users log in to the systems 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
Organization
Job Title

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

Employees
Vendor/Suppliers/Contractors
Former NIAID employees

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

Identification and authentication for access to the system and specific research data sets.

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

Audit trail information for source sample records.

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

42 U.S.C. 241, Research and Investigation

42 U.S.C. 285f, National Institute on Allergy and Infectious Diseases

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.

09–25–0200 Clinical, Basic and Population-based Research Studies of the National Institutes of

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

NIH research activities are exempt from an OMB Information Collection Number through Public Law 114-255 - 21st Century Cures Act, Section 2035: Exemption for the National Institutes of Health from the Paperwork Reduction Act requirements.

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.

No prior notice is provided. PII is sourced from the NIH Enterprise Directory (NED) or the NIAID Employee Assignment Registry (NEAR), which maintains their own PIA, including all legal authorities. Users are notified of the collection as part of the NIH onboarding processes.

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.

No option to opt out as access is required in order for the user to perform their duties.

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

Consent is not required. Employee PII is derived from the NIH Enterprise Directory (NED) or the NIAID Employee Assignment Registry (NEAR), which maintains their own PIA, including all legal authorities. If the user leaves NIH, the user application account is disabled, but the account and associated PII is retained for audit trail purposes.

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.

No process is in place. Employee PII is obtained from NED or NEAR, which maintains their own PIA, including all legal authorities. Usage is for identification/authentication, association to a research or sample record, and retained for sample audit trail purposes.

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

No processes are required. The applications are dependent on the information from NED or NEAR, which maintains their own PIA, including all legal authorities. No revalidation of the PII is required.

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 or group-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.

Access to PII is assigned to personnel based upon current job responsibilities. A NIH IAM Systems account login is required to gain access to the applications.

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).

NIH provided role-based training for administrators and Privileged Users.

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 throughout the life of the system in accordance with the following NIH Record Schedule:
- 01-003, Records of All Other Intramural Research Projects (Disposition Authority Agency (DAA) -0443-2012-0007-0003). Cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer. Destroy 7 years after cutoff.

- 07-203, System access records. Systems not requiring special accountability for access (DAA-GRS-2013-0006-0001). Destroy when business use ceases.

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

Administrative Controls: Includes performing background checks, completing security and privacy training, limiting access to NIH personnel from participating laboratories, and implementing role-based access for authorized users.

Technical Controls: Access to the system is controlled by NIH log-in which authenticates the user prior to granting access. Access level and permissions are controlled by the system and based on user, role, organizational unit, and status of the report. All servers have been configured to remove all unused applications and system files and all local account access except when necessary to manage the system and maintain integrity of data.

Physical Controls: The on-prem servers supporting FERMS and VHICL-IMS reside in the NIAID Research Development and Compute Facility (RDCF) where policies and procedures are in place to restrict access to the machines. This includes guards at the main entrance and Personal Identity Verification (PIV) card readers at the entrance to the RDCF. DIADEM resides on the Monarch platform. The physical safeguards are inherited from Amazon Web Services (AWS) which houses the system in a Federal Risk and Authorization Management Program (FedRAMP) certified facility.