US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/30/2025

OPDIV:

NIH

Name:

Lots of Boxes on Shelves Network

PIA Unique Identifier:

P-9224723-106527

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)?

No

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The Lots of Boxes on Shelves (LoBoS) is used by researchers in the Laboratory of Computational Biology (LCB), Division of Intramural Research, National Heart, Lung, and Blood Institute (NHLBI) to run computational simulations. The system supports both internal lab members as well as a few outside collaborators, typically former lab members or users at academic institutions working on joint projects.

The system is hosted in two computer rooms on the main NIH campus. One is completely managed by lab staff while the other is in leased space that is managed by the Center for Information Technology (CIT).

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

Simulations are basic biological processes and involve no clinical information or patient data. System data is for internal use of NHLBI staff and collaborators, data generated is computer-based modeling and results are eventually published.

Users accessing this system use specific login which include username, password, name and email of the user.

Administrators login 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 LoBoS is used by researchers in the LCB, Division of Intramural Research, NHLBI to run computational simulations. The system supports both internal lab members as well as a few outside collaborators, typically former lab members or users at academic institutions working on joint projects.

The system is hosted in two computer rooms on the main NIH campus, one is completely managed by lab staff while the other is in leased space that is managed by the CIT.

Simulations are basic research and involve no clinical information or patient data. System data is for internal use of NHLBI staff and collaborators, data generated is computer-based modeling, results are eventually published.

Users accessing this system use specific login which include username, password, name and email of the user.

Administrators login using the NIH IAM Services which maintains its own unique PIA on record, including all legal authorities documented.

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
Password
Username

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

Employees
Business Partner/Contacts (Federal/state/local agencies)

How many individuals' PII is in the system?

<100

For what primary purpose is the PII used?

For login authentication

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

N/A

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

5 U.S.C. 301; Information Technology Management Reform Act of 1996 (Pub. L. 104-106, sec. 5113); Electronic Government Act (Pub. L. 104- 347, sec. 203); Government Paperwork Elimination Act (Pub. L. 105-277, sec. 1701, 44 U.S.C. 3504); Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, Aug. 27, 2004; Federal Property and Administrative Act of 1949, as amended

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.

SORN 09-90-0777 - Facility and Resource Access Control Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Online

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

N/A. Information is not solicited. Personally Identifiable Information (PII) is used for login only.

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.

N/A

Describe the procedures for accounting for disclosures.

Audit Logs are used.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

Emails are sent for their personal information or collected in person in the Lab.

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.

Users cannot gain access to the system if they opt out from giving their information.

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

A mass email is sent to individuals whose PII is in the system when there is a major change.

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 may contact their Institute, Center, Office Privacy Coordinator or the NIH Senior Official for Privacy at Privacy@mail.nih.gov.

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

Periodic audits are conducted to ensure the data's integrity, availability, accuracy and relevancy. The system produces reports for review by system administrators, system owners and business owners.

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.

Specific NIH IAM login credentials are required to access the stored PII.

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).

Administrators and Privileged Users require additional training specific to their roles and responsibilities.

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 retained and disposed of under the authority of the NIH Records Retention Schedule.

Item: 07-203 System access records. Systems not requiring special accountability for access.

These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
Includes records such as: user profiles,log-in files,password files,audit trail files and extracts, system usage files cost-back files used to assess charges for system use

Exclusion 1. Excludes records relating to electronic signatures.

Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.

Systems not requiring special accountability for access.
These are user identification records generated according to preset requirements, typically system generated. A system may, for example, prompt users for new passwords every 90 days for all users.

Disposition: Destroy when business use ceases.

DAA-GRS-2013-0006-0003

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

Physical Controls: The information technology (IT) hardware used to host protected information is located in two secured data facilities. Each facility is only open to authorized personnel whose access is monitored by locking doors with badge readers for both ingress and egress. Each discrete ingress and egress event is logged. The facilities are under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software is segregated from default commodity public networks to prevent unauthorized or malicious access. Access controls lists and event logs are maintained and monitored to detect unauthorized, suspicious or malicious activity. Access lists are restricted to approved IT technical personnel. Two factor authentication must be used for access. File integrity and auditing software are employed on hardware.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria for Public Trust positions. All personnel have taken mandatory security and privacy training classes and annual refreshers. Administrative personnel accessing these systems use privileged and separate accounts for administrative access.

Identify the publicly-available URL:

https://help.lobos.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?

No

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?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null