US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/08/2024

OPDIV:

NIH

Name:

NIBIB Software, Tutorials, Protocols, and Workshops (DMAS-LCIMB)

PIA Unique Identifier:

P-1451238-299505

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?

Existing

Does the system have Security Authorization (SA)?

Yes

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

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

The web application was originally hosted on the Center for Information Technology (CIT) Shared Services Infrastructure. It was converted from Hyper Text Markup Language (HTML) to the Drupal format and is now hosted in the Acquia cloud.

Describe the purpose of the system.

The Software, Tutorials, Protocols, and Workshops, provided by the National Institute of Biomedical Imaging and Bioengineering (NIBIB) Dynamics of Macromolecular Assembly group of the Laboratory of Cellular Imaging and Macromolecular Biophysics (DMAS-LCIMB), provides a means for the distribution of software and other tools related to the biophysical techniques developed under the DMAS-LCIMB.

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

To access DMAS-LCIMB, users register by providing the following information:
Username

Email Address
Photographs (optional)

Administrators (admins) and developers requiring access 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 store 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.

Software, Tutorials, Protocols, and Workshops from DMAS-LCIMB website is hosted by the Center for Information Technology (CIT). Its purpose is to provide a means for the distribution of software and other tools related to the biophysical techniques developed within NIBIB's DMAS-LCIMB.

The website collects the following personally identifiable information (PII) during the account registration process:
Username
Email address
Photograph (optional)

Admins log in to the system 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.

Photographic Identifiers
E-Mail Address
Username

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

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The PII is used to create a user account for access to the site.

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); Paperwork Reduction Act of 1995 (44 U.S.C. ch. 35); Government Paperwork Elimination Act (Pub. L. 105-277, sec. 1701, 44 U.S.C. 3504)

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.

09-90-0777 Facility and Resource Access Control Records

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Non-Governmental Sources

Private Sector

Identify the OMB information collection approval number and expiration date

N/A

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.

Notification is posted on the website when users opt in to create an account.

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.

Submission of the information is voluntary when requesting an account. If they choose not to create and account, they are not able to access the information.

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

To date, no major changes have occurred to the system that necessitated notifying the user. In the event of a major change, the email address will be used to contact individuals.

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 email info@nibib.nih.gov or contact the NIH Senior Official for Privacy.

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

The NIH Information Technology (IT) Privacy Program requires systems to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks, and interconnected systems.

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.

Access to PII is assigned to personnel based upon current job responsibilities. The system uses specific login information to assign permissions/user roles which is considered PII.

Administrators and developers log in to the sites using NIH IAM services, which maintains its own unique PIA on record, including all legal authorities documented.

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.

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.

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.

The NIH Security Awareness Training course satisfies this requirement. According to NIH policy, all personnel who use NIH applications must complete security awareness training annually. There are five categories of mandatory information technology (IT) training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness).

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

Web Developers 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.
System access records.
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: IT hardware used to host protected information is located in a secured datacenter facility. The 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 facility is under 24-hour surveillance by facilities security for security and environmental hazards.

Technical Controls: IT hardware and software are 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 authentications 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 sites use privileged and separate accounts for administrative access.

Identify the publicly-available URL:

https://sedfitsedphat.prod.acquia-sites.com/

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