US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/04/2025

OPDIV:

NIH

Name:

NLM Data Center

PIA Unique Identifier:

P-6347532-865712

The subject of this PIA is which of the following?

General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

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

Significant System Management Change

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

Since the last Privacy Impact Assessment (PIA) there has been a system owner change and Sequence Read Archive (SRA), a minor application, was moved to the Biomedical and Biological Information System, and is no longer a part of the National Library of Medicine (NLM) Data Center boundary.

Describe the purpose of the system.

The National Library of Medicine (NLM) Data Center (DC) (NLMDC) General Support System (GSS) houses minor applications that carry out the NLM mission-enabling biomedical research, supporting health care and public health. The NLMDC applications act as System backup, Incident Response, Critical Infrastructure Monitoring, System Equipment Monitoring, Service Desk Support, Data Recovery/Continuity of Operations Plan, and Physical and Environmental Security. Minor applications within NLMDC have unique and specific privacy impact assessments (PIAs) which

address the type of information the specific system will collect, maintain, store, and share, including personally identifiable information (PII). Each minor application will list the GSS' Universally Unique Identifier (UUID) within their respective PIAs.

Minor applications include:

Access Global Unique Device Identification (AccessGUDID) is a web portal to make medical device identification information available to individuals.
DailyMed provides high-quality information about marketed drugs.
Digital Repository provides preservation and access to digitized versions of NLM's historical medical materials.
DOCLINE is an Interlibrary Loan (ILL) & document delivery system which allows libraries and individuals to transmit requests for biomedical-related literature.
Medical Subject Headings (MeSH) is a thesaurus for indexing articles from the world's leading biomedical journals for the MEDLINE/PubMed database.
MedlinePlus (M+) is a list of authoritative health information sources from NIH and other organizations.
RxNorm Editing System is an editing application used for the creation and maintenance of the RxNorm drug vocabulary.
Serials Extract File (SEF) is a database containing Serials bibliographic information that is updated daily from the Voyager database.
Unified Medical Language System (UMLS) is a set of files and software that brings together health and biomedical vocabularies and standards to enable interoperability between computer systems.
UMLS Metatheasaurus License provides access for users to browse, search, and download health data standards and terminologies.
Value Set Authority Center (VSAC) is used for the storage and retrieval of value sets through the web.

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

NLM Data Center is a GSS consisting of computers, routers, and information technology (IT) hardware. It does not collect, maintain, disseminated information, or PII.

However, the following applications/systems reside under the GSS security boundary and collect the following information.

PII is not collected, but does contain the following information:
AccessGUDID - medical device information
BLAST - annotated collection of all publicly available nucleotide sequences
DailyMed - medication product label information
dbGaP - phenotypic data, study documentation, genotypes, and statistical results
Digital Repository - digitized films, books, and IndexCat (Category) citations
MeSHContains vocabulary thesaurus
M+Contains consumer health educational information
PubChem is a chemistry database
RxNorm - generic and branded drug names
SEF - Serials information and data
SRA - sequence data
UMLS - inversion data files
VSAC - value sets for standardized medical terminology

The following contains data (specified) as well as contact information (name, email address, phone number, mailing address, title and/or organization/affiliation):
GenBank - Nucleotide data

MEDLARS: Bibliographic data
NBTS
DOCLINE
GTR
ClinicalTrials.gov
UMLS Metatheasaurus License

PubMed and PubCentral users log with their 'local' login credentials using InCommon.

Each system maintains their own PIA, with all legal authorities documented.

NIH employees accessing these systems login using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique 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.

NLM Data Center is a GSS consisting of computers, routers, and IT hardware. It does not collect, maintain, disseminated information, or PII.

However, the following applications/systems reside under the GSS security boundary and collect the following information.

PII is not collected, but does contain the following information:
AccessGUDID - medical device information
DailyMed - medication product label information
Digital Repository - digitized films, books, and IndexCat citations
MeSH - Contains vocabulary thesaurus
M+ - Contains consumer health educational information
RxNorm - generic and branded drug names
SEF - Serials information and data
UMLS - inversion data files
VSAC - value sets for standardized medical terminology

The following systems contains contact information (name, email address, phone number, mailing address, title and/or organization/affiliation) and are accounted for under their own unique PIA:

DOCLINE
UMLS Metatheasaurus License

Each system maintains their own PIA, with all legal authorities documented and will list the NIH Data Center's GSS' UUID within their respective PIAs.

NIH employees accessing these systems 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
Mailing Address
Phone Numbers
Title,organization/department affiliation

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

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

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The NLMDC and its minor applications use PII for the following purposes:

Functional access and credentials for logging into applications.
Provide contact information regarding partnered laboratories, as well as internal and external partners.

Contact information for requesting information and assistance
to fulfill requests for medical literature.
Sign up for email updates and notifications.

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

For DOCLINE, copied library and patron data may be used to test the ongoing development of the system in a test bed environment.

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

42 U.S.C. section 286, 42 U.S.C. § 282(i) and (j)), 44 U.S.C. Sec. 2904, 42 U.S.C. 241.

Section 402(i) and 402(j) of the Public Health Service Act.

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.

09-25-0005, Administration: Library Operations and NIH Library User Identification (ID) File

09-90-1901: Correspondence, Customer Service, and Contact List Records.

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Other Federal Entities

Other Federal Agencies

State or Local Agencies

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

For Federal Entities residing in the NLMDC, information is not solicited. Submission of an individual's PII is voluntary and not required for use of the systems. The collection of minimum PII is used as creation and membership into applications and/or for sign up of mailing lists to stay up to date on system changes and additions.

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.

Not applicable. The only PII that individuals external to NIH have access to are library information and limited contact information associated with NLM library documents.

Describe the procedures for accounting for disclosures.

Disclosure requests are to be made to the System Managers to determine if the record exists and if the requester has permission to access the record(s).

When a request for an accounting is received, there are audit logs to allow the system owner to provide that information.

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

Individuals are notified that their personal information will be collected through a collection of processes dependent on each minor application's applicability to the Privacy Act and other laws and regulations. These processes include:

Code of conduct statements.
Providing individuals with the Office of Management and Budget (OMB) Burden Statement.
Privacy Act Statements and Notices.
Confirmation Emails verifying an individuals' request to sign up.
Terms and conditions of use.

Specific notification processes are outlined in each minor application's PIA.

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.

All minor applications within the NLMDC maintain their own PIAs, including specific processes for opt-out options and legal authorities.

While unsubscribing or requesting removal of an individual's PII is possible for all applications, doing so would result in individuals not being able to participate in collaboration and use of the minor applications.

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

All minor applications within the NLMDC maintain their own PIAs, including specific processes for notification and consent when major changes occur and legal authorities.

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.

All minor applications within the NLMDC maintain their own PIAs, including specific processes for notification and consent when major changes occur and legal authorities.

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

All minor applications within the NLMDC maintain their own PIAs, including specific processes for periodic reviews of PII and legal authorities.

Processes for periodic reviews of PII in minor applications within NLMDC include:
periodic data integrity audits
regular security scans and backups
annual reviews of records

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.

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.

Access to PII is assigned to personnel based upon current job responsibilities. An NIH IAM System 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.

All personnel who manage or operate NIH applications must successfully complete annual security 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).

For DOCLINE, system developers are trained in security scanning and vulnerability management.

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 10-101 - Administrative records maintained in any agency office.
Administrative records maintained in any agency office. Records accumulated by individual offices that relate to routine day-to-day administration and management of the office rather than the mission-specific activities for which the office exists, excluding records scheduled elsewhere in the General Retention Schedule (GRS) such as timekeeping and procurement.
Disposition: Destroy when business use ceases. DAA-GRS-2016-0016-0001

Item 07-204 - System access records. Systems 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.
Disposition: Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. DAA-GRS-2013-0006-0004

Item 07-201 - Systems and data security records. These are records related to maintaining the security of information technology (IT) systems and data.
Records outline official procedures for securing and maintaining IT infrastructure and relate to the specific systems for which they were written. This series also includes analysis of security policies, processes, and guidelines, as well as system risk management and vulnerability analyses.
Disposition: Destroy 1 year(s) after system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. DAA-GRS-2013-0006-0001

Item 01-003 - Records of All Other Intramural Research Projects.
These records do not meet the retention criteria for Item I-0001 - Records of Intramural Research Records or for Projects of Historical Significance, or Item I-0002 - Research Records that Support Intellectual Property Rights.
Disposition: Cut off annually at termination of project/program or when no longer needed for scientific reference, whichever is longer. Destroy 7 years after cutoff. DAA-0443-2012-0007-0003

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

Administrative Controls: System users are approved by NLMDC's management for access based on their technical/functional role in administering, developing, and supporting the NLMDC's daily job functions.

Technical Controls: Access to the system is controlled by NIH IAM login which authenticates the user before 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 the integrity of data.

Physical Controls: The servers reside in the NLM Data Center where policies and procedures are in place to restrict access to the machines. This includes biometric equipment such as Iris scanners, as well as cameras that monitor all the doors.

Identify the publicly-available URL:

https://accessgudid.nlm.nih.gov/

Https://dailymed.nlm.nih.gov/dailymed/

http://collections.nlm.nih.gov
https://www.nlm.nih.gov/mesh/
MedlinePlus English: https://medlineplus.gov/
MedlinePlus Spanish: https://medlineplus.gov/esp/
https://docline.gov
https://uts.nlm.nih.gov/uts/
https://vsac.nlm.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