US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/30/2025

OPDIV:

NIH

Name:

UMLS Metathesaurus License

PIA Unique Identifier:

P-6951862-165605

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 System Owner was updated, Business Parnter/Contacts were added. Direct Contractors have access to personally identifiable information (PII). Web technologies were updated.

Minor systems under the National Library of Medicine (NLM) Data Center (NLMDC) were moved under the Biomedical and Biological Information System (BBIS) during the NLM system realignment to better fit into the management of the systems.

Describe the purpose of the system.

The Unified Medical Language System (UMLS) Metathesaurus License provides access for users to browse, search, and download health data standards and terminologies provided by the National Library of Medicine (NLM). The system collects first name, last name, email address, postal address, city, country, postal/zip code, phone number, their affiliation, primary activity of institution/organization, and role of institute/organization.

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

The system collects first name, last name, email address, mailing address country, phone number, their affiliation, primary activity and role of their institute/organization, and user credentials (login and password).

Appendix 1 of the UMLS Metathesaurus list all source vocabularies in UMLS Metathesaurus and the contact information for the owners of the source vocabularies. This information is public information and not the personally identifiable information (PII) of UMLS Metathesaurus License users.

Those requiring administrative access to this system log in using the NIH Identity, Credential, and Access Management (IAM) Services which maintains its own unique privacy impact assessment (PIA) on record, with 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 collects unique user credentials and stores them in an encrypted format. The IAM Service is 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 UMLS Metathesaurus License provides access for users to browse, search, and download health data standards and terminologies provided by the NLM.

The system collects first name, last name, email address, mailing address country, phone number, their affiliation, primary activity and role of their institute/organization, and user credentials (login and password).

Appendix 1 of the UMLS Metathesaurus list all source vocabularies in UMLS Metathesaurus and the contact information for the owners of the source vocabularies. This information is public information and not the PII of UMLS Metathesaurus License users.

Those requiring administrative access to this system log in using the NIH IAM Services which maintains its own unique PIA on record, with 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
Organizational Affiliation and Country
Organizational Role and primary activity
User credentials

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?

50,000-99,999

For what primary purpose is the PII used?

The primary purpose is to verify user identity for access to copyrighted health data standards and terminologies provided by the NLM.

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

Not applicable.

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.

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the DOC

Other HHS Operat

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

NA. UMLS Metathesaurus License does not solicit information from the public. Submission of an individual's email address is voluntary and not required for use of UMLS Metathesaurus License.

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.

There are currently no information sharing or disclosure agreements in place.

Describe the procedures for accounting for disclosures.

Disclosure requests are to be made to the System Manager 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.

Personally identifiable information (PII) is voluntarily submitted by individuals. It is understood the individual must provide their information to accept the terms of the UMLS Metathesaurus License.

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.

To access health data standards and terminologies provided by the National Library of Medicine (NLM), individuals must opt-in to the collection of their Personally Identifiable Information (PII). Users can opt-out up front or submit an email request to have their information deleted at any time; however, they will no longer have access to the data.

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

Individuals will be emailed multiple times with at least 3 months lead time before any changes to the use or collection of their information are implemented.

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 who have concerns about the accuracy of their information can contact the UMLS team or revise the information directly through the UMLS Metathesaurus License system.

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

Individual records are manually reviewed upon submission. System records are routinely checked for integrity, availability, and accuracy. An annual review of records ensures that irrelevant and inactive records are purged from the system.

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.

Access to PII is assigned to personnel based upon current job responsibilities. An IAM account login is required to gain access to the stored PII data.

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.

Administrative rights to access individuals' information must be requested from and approved by the project lead. Users with administrative rights can search for individual records but cannot access all individuals' information in bulk.

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).

Not applicable.

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 Records Schedule (GRS) such as timekeeping and procurement.
Disposition: Destroy when business use ceases. DAA-GRS2016-0016-0001

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/information technology (IT) administrative purposes to ensure a continuity of security controls throughout the life of the system. DAA-GRS-2013-0006-0001

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

Administrative Controls: System administrators are approved by for access based on their technical/functional role in administering, developing, and supporting UMLS Metatheasaurus' daily job functions, and UMLS Metatheasaurus administrators perform periodic reviews to assure users adhere to system policies.

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 servers reside in the Center for Information Technology (CIT) Computer Room where policies and procedures are in place to restrict access to the machines. This includes guards at the front door and entrance to the machine room.

Identify the publicly-available URL:

https://www.nlm.nih.gov/research/umls/index.html

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