US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/22/2025

OPDIV:

NIH

Name:

NLM Data Center: MEDLARS: DOCLINE

PIA Unique Identifier:

P-3859703-459581

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.

This validation is intended to refresh content. There have been no substantial changes since the last assessment.

Describe the purpose of the system.

The system enables health professionals and the public to obtain the medical/health information they need from medical libraries. It is an Interlibrary loan (ILL) and document delivery system which allows libraries and individuals to transmit requests for biomedical-related literature.

DOCLINE is available to participating federal and state libraries, hospitals, medical schools and research institutes.

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

The following information is collected:
Contact information (name, address, email, phone number) for libraries, and library staff, as well as information about library services, policies, and journals available at the library is collected.

Library patron information (name, email, mailing address, username, and login) is stored in the system for use by the libraries serving their needs.

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 system enables health professionals and the public to obtain the medical/health information they need from medical libraries. It is an IILL and document delivery system which allows libraries and individuals to transmit requests for biomedical-related literature.

Contact information (name, address, email) for libraries, and library staff, as well as information about library services, policies, and journals available at the library are collected. Library patron information (name, email, mailing address, username, and login) is stored in the system for use by the libraries serving their needs. National Library of Medicine (NLM) does not use the collected patron information.

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.

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
Login and password
Library services, policies, and journals available

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

Employees
Public Citizens
Library staff

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

To fulfill requests for medical literature.

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

Copied library and patron data may be used to test the ongoing development of the systemin a test bed environment. Data may also be used for research purposes such as usage of topics. The data can also be used for billing purposes.

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

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 I.D. 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 Operating Div

State/Local/Tribal

Foreign

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Not Applicable. DOCLINE does not solicit the public for information. Sign up is voluntary and is only used to allow the creation and membership into the NLM Library for users.

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 no sharing agreements in place.

Describe the procedures for accounting for disclosures.

Disclosures must be done in writing to the System Manager, along with being notarized. Audit logs are kept to account for disclosures.

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

Links providing access to Privacy statements are displayed to the user before they before they register to use the system and again before log into the system.

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.

There is no opt-out procedure. If an individual would no longer like their information kept in the system, they may request that it is removed. However, in doing so, the individual will no longer be granted access to DOCLINE.

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

Users are notified via messages displayed in the system interface, as well as listserv postings.

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.

User concerns are investigated by DOCLINE administrators and precautions are taken to safeguard data.

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

Regular security scans and back ups are completed and any vulnerabilities are addressed. Users are prompted to keep their information up to date.

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.

Periodic review of system users' roles are done to assure access is current with user's technical/functional role in administering, developing, and supporting the daily job functions of the DOCLINE.

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.

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).

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 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: Temporary: Destroy 1 year after the 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 users are approved by DOCLINE's management for access based on their technical/functional role in administering, developing, and supporting DOCLINE's daily job functions, and DOCLINE 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: System is in cloud and is physically protected by Amazon Web Services (AWS) policies and procedures. The ADM servers resides in the NLM Data Center where policies and procedures are in place to restrict access to the machines. This includes biometric access at the front door and entrance to the data center.

Identify the publicly-available URL:

https://docline.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.

Other technologies that do not collect PII:

Google Analytics 4

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