US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/30/2025

OPDIV:

NIH

Name:

Alma/Primo

PIA Unique Identifier:

P-9670617-531469

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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?

No

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

Alma/Primo is a library system for the organization of print and electronic library resources.

Alma is the backend part of the system that library staff will use to acquire, catalog, organize, and represent NIH Library's physical and electronic holdings (books, journals, and other media). Alma creates a file of bibliographic records which it exports to Primo.

Primo provides the front end interface for patrons for their day-to-day operations to search and request services for library resources. It's the public facing discovery aspect of the system that staff and researchers across the NIH, Centers for Medicare & Medicaid Services (CMS), and the Department of Health and Human Services (HHS) will use for research purposes.

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

Alma stores the following personally identifiable information (PII): First and last name, email address in relation to creating a unique password of system administrators and library staff, phone number,

mailing address (building and room number).

Primo does not collect, maintain and/or share PII.

The PII retained in Alma is used primarily for communicating with library patrons that have library materials checked out. Patrons are research associates and not members of the public. The PII of a small number of Division of Library Services (DLS) staff is used to contact users (for communicating issues, sending reports and managing passwords).

Only DLS staff will be logging in and using Alma. They log in to it 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.

Alma/Primo is a library system for the organization of print and electronic library resources.

Alma is the backend part of the system that library staff will use to acquire, catalog, organize, and represent NIH Library's physical and electronic holdings (books, journals, and other media). Alma creates a file of bibliographic records which it exports to Primo.

Primo provides the front end interface for patrons for their day-to-day operations to search and request services for library resources. It's the public facing discovery aspect of the system that staff and researchers across the NIH, CMS, and HHS will use for research purposes.

Alma stores the following PII: First and last name, email address (in relation to creating a unique password of system administrators and library staff), phone number, mailing address (building and room number).

Primo does not collect, maintain and/or share PII.

The PII retained in Alma is used primarily for communicating with library patrons that have library materials checked out to them. Patrons are research associates and not members of the public. The PII of a small number of DLS staff (who administer the system and perform library work) is used to contact users (for communicating issues, sending reports and managing passwords).

Only DLS staff will be logging in and using Alma. They log in to it 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
passwords

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?

5,000-9,999

For what primary purpose is the PII used?

The primary purpose of PII collected by Alma is for identification and authentication purposes.

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 and 302, 44 U.S.C. 3101
and 3102

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: 09-90-1901 HHS Correspondence, Comment, Customer Service and Contact List Reocrds.

SORN: 09-25-0216, Administration: NIH Electronic Directory, HHS/NIH

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Email

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Non-Governmental Sources

Other

Identify the OMB information collection approval number and expiration date

N/A. Alma-Primo does not solicit PII.

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.

The personal information for NIH staff is downloaded from the NIH Enterprise Directory (NED). Information that is pulled from NED is voluntarily submitted and entered by an Administrative Officer or by the employee. NED has its own approved PIA on record, including all legal authorities documented.

All persons who enter in business relationships with NIH are fully informed in writing prior to the beginning of the transaction that PII is required in order to proceed.

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 access Alma/Primo 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.

The information collection for NIH staff flows from NED and if an Administrative Officer (AO) makes any changes to that system, the user will receive an email message.

Registered users will receive an email if there is major changes.

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 can contact the NIH Information Technology (IT) Service Desk.

NIH staff may also contact the NED team directly at nedteam@mail.nih.gov or their servicing AO.

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 PII downloaded from NED is reviewed when HHS Personal Identity Verification (PIV) cards are renewed. Alternatively, individuals have the option to conduct ad hoc reviews of their own PII through NED Self Service. Patron records that have expired will be purged from the system periodically.

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 according to 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.

According to NIH policy, 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).

N/A

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 08-301: Library administrative records.
Description: Records documenting a library's planning and management. Records may document library policies, procedures, and statistics. Includes records such as policies and procedures for developing collections, acquisitions, patron privacy, loans, and restricting library material and quick guides to library databases and resources , topical or customized reading lists, and bibliographies.
Disposition: Destroy when 3 years old or 3 years after superseded or obsolete, whichever is applicable. Longer retention is authorized for business use.
Disposition Authority: DAA-GRS-2015-0003-0001

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

Physical Controls: The IT hardware used to host protected information is located in a secured data center 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 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.