US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/09/2025

OPDIV:

NIH

Name:

National Institute of Allergy and Infectious Diseases Document Records Process Automation System Authorization Boundary

PIA Unique Identifier:

P-1226593-511005

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?

No

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.

N/A

Describe the purpose of the system.

The National Institute of Allergy and Infectious Diseases (NIAID) Document Records Process Automation System (NDRPAS) provides an extensive set of tools that quickly and easily addresses commonly entrenched enterprise content management challenges of effectively storing, classifying, updating, finding, retrieving, and tracking of documents, records, and cases.

NDRPAS is used to provide document management within a central location. NDRPAS stores data which consists of four elements: documents, database metadata, full text index, and backup of the full text index, and maintains the records of an organization from the time they are created until disposal.

NDRPAS, along with its three subsystems Enterprise Documents and Records Management Systems (EDRMS), Validated EDRMS (VEDRMS), and EDRMS Shared Services (ESS) collects, maintains and shares grant-related data, contract-related data, scientific research data, administrative information, training, and standard operating procedures (SOPs).

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

The primary purpose of the collected personally identifiable information (PII) and sensitive information stored within the NDRPAS repository is to support the specific business and mission requirements within NIAID. Examples of such support processes involve storing PII information related to Human Resources (HR) record keeping, clinical data and management, and other functions integral to support NIAID's mission.

Original correspondence is scanned or saved within the system. Correspondence may contain the following PII: Names, Date of Birth, Social Security Numbers, Medical records and notes, Phone numbers, Date of Birth, Email Addresses, Resumes, and Government Identification Numbers, such as drivers license, passport and military ID numbers. There is no process in place to notify, obtain additional information, or provide further consent after the correspondence has been received.

NDRPAS does not solicit or collect additional information for a database. The originator/correspondent voluntarily sends PII in the correspondence they authored and NDRPAS only contains an image of the document originally submitted. NDRPAS does not manipulate the information for another use.

Users log in to the systems 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 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.

The National Institute of Allergy and Infectious Diseases (NIAID) Document Records Process Automation System (NDRPAS) provides an extensive set of tools that quickly and easily addresses commonly entrenched enterprise content management challenges of effectively storing, classifying, updating, finding, retrieving, and tracking of documents, records, and cases.

NDRPAS is used to provide document management within a central location. NDRPAS stores data which consists of four elements: documents, database metadata, full text index, and backup of the full text index, and maintains the records of an organization from the time they are created until disposal.

NDRPAS, along with its three subsystems Enterprise Documents and Records Management Systems (EDRMS), Validated EDRMS (VEDRMS), and EDRMS Shared Services (ESS) collects, maintains and shares grant-related data, contract-related data, scientific research data, administrative information, training, and standard operating procedures (SOPs).

The primary purpose of the collected PII and sensitive information stored within the NDRPAS repository is to support the specific business and mission requirements within NIAID. Examples of such support processes involve storing PII information related to Human Resources (HR) record keeping, clinical data and management, and other functions integral to support NIAID's mission.

Original correspondence is scanned or saved within the system. Correspondence may contain the following personally identifiable information (PII): Names, Date of Birth, Social Security Numbers, Medical records and notes, Phone numbers, Date of Birth, Email Addresses, Resumes, and Government Identification Numbers, such as drivers license, passport and military ID numbers. There is no process in place to notify, obtain additional information, or provide further consent after the correspondence has been received.

NDRPAS does not solicit or collect additional information for a database. The originator/correspondent voluntarily sends PII in the correspondence they authored and NDRPAS only contains an image of the document originally submitted. NDRPAS does not manipulate the information for another use.

Users log in to the systems 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 stores them in an encrypted format. The IAM Services are an essential service which facilitates and governs network access to various resources.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Social Security Number
Date of Birth
Name
Driver's License Number
E-Mail Address
Phone Numbers
Medical Records Number
Medical Notes
Passport Number
Login usernames and passwords
Other - The correspondences may contain personally identifiable information (PII) .
Resumes
Contract related data
Military IDs

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

Employees
Business Partner/Contacts (Federal/state/local agencies)
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

The primary purpose of the collected PII and sensitive information stored within the NDRPAS repository is to support the specific business and mission requirements within NIAID. Examples of such support process involve storing PII information related to Human Resources (HR) record

keeping, clinical data and management, and other functions integral to support NIAID's mission.

The system uses NIH Login credentials (username and Password) for authentication purposes and maintains the user name in order to ensure the establishment of use and viewing rights in the system.

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. 241, 248; 44 U.S.C. 241, 248, 282, and 284; 42 U.S.C. 241, 242, 248, 281, 282, 284, 285a, 285b, 285c, 285d, 285e, 285f, 285g, 285h, 285i, 285j, 285l, 285m, 285n, 285o, 285p, 285q, 287, 287b, 287c, 289a, 289c, and 44 U.S.C. 3101.

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.

09-25-0200, Clinical, Basic and Population-based Research Studies of the National Institute of

09-25-0099, Clinical Research: Patient Medical Records

Identify the sources of PII in the system.

Government Sources

Within OpDiv

Identify the OMB information collection approval number and expiration date

Not applicable.

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.

NDRPAS is the custodian of documents within the system. The business owner of each specific application or repository is responsible for notifying individuals about PII collection before the information is entered into NDRPAS. Prior notice is provided outside of NDRPAS.

If NDRPAS users do not want to provide their user credentials, they are unable to gain access to 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.

The business owner of the application or repository is responsible for providing notification to users of the requirements for PII collection and this process is conducted outside of NDRPAS' use. The only method of opting out of the PII collection is for the individual to choose not to participate.

Because the information uploaded is an image of the original content, NDRPAS does not have the ability to utilize the PII that is stored within the system. The business owner of the application or repository has their own process for providing notification of PII collection and how individuals may opt out. This takes place outside of NDRPAS through other processes.

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

The business owner of the application or repository within NDRPAS is responsible for notifying and obtaining consent of individuals when major changes occur. Such activity is conducted outside of the NDRPAS system.

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.

For the NDRPAS systems and repositories that include PII, the business owner of the application or repository is responsible for resolution of individual concerns about PII in NDRPAS. Such activity is outside of NDRPAS.

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

For the NDRPAS system and repositories that include PII, the business owner of the application or repository is responsible for periodic reviews of PII in NDRPAS to ensure the data's integrity, availability, accuracy and relevancy. Such activity is conducted outside of the NDRPAS 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.

Other than end users (repository/application business owners and authorized users of each repository/application), the only others with access to PII within NDRPAS are the various system administrators. System administrators require access to all data and documents to perform their functions. Each type of administrator is granted access to PII documents when they are given administrative rights and responsibilities in their area of expertise by their NIAID manager for products, databases, servers, storage and/or other system peripherals of NDRPAS.

If documents with PII are accessed, an audit trail tracks all activities, including who accessed the information. In the Content Server Commercial Off The Shelf (COTS) product, the administrator role has full system access, to include PII by definition. Database administrators require access to databases that may include PII data to perform their functions.

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.

The NDRPAS system and applications have a Community, Information and Security (CIS) Model which formally delineates the type of access each user or group of users have to information stored in the application or repository. For applications and repositories with PII data contained in resumes, all user groups have access to the data.

For applications and repositories with PII data about NIAID employees, only a pre-authorized group of users with the need to access information about an employee has access to the PII.

For applications and repositories with PII data about patients or public citizens, only a pre-authorized group of users with the need to access information about such people has access to the PII. Security controls are in place to limit access based on least privilege.

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).

When a user is given authorization to a specific NDRPAS application or repository, the business owner of that application or repository ensures that each user is trained in its use, including access controls and restrictions.

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.

Information stored and maintained in the NDRPAS are retained and disposed under the authority of the (NIH Intramural Records Schedule, Item I-0003: Records of All Other Intramural Research Projects.) These are temporary records, cut off at termination project/program or when no longer needed/required for scientific referencing, whichever is longer or destroyed 7 years after cutoff. [Disposition Authority Agency: DAA-0443-2012-0007-0003]

Login /Systems Access Records are retained and disposed of under the authority of the (NIH General Records Schedule, Section 07-204 Information Systems Security Records.) These are temporary records. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.
[Disposition Authority Agency: DAA-GRS-2013-0006-0004]

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

Each repository/application within the NDRPAS has access control limitations assigned to them through administrative controls. The control is the formal process of provisioning and granting role-based access rights to each NDRPAS repository/application and each potential user. Role assignments are based on the Community, Information and Security (CIS) Model, which formally delineates the type of access permissions a user is given based on the role/group name. The role must be requested and approved by the Business Owner before the user will be able to see the information within the repository/application. If a user does not have the role assignment necessary to access the information within, the user will not be able to see that it exists. Lastly, additional security training is required for all administrators with access to PII. This training is targeted explicitly for the proper security requirements for safeguarding PII.

Technical controls safeguards include restricting access to authenticated users via Federal Information Processing Standard (FIPS) 140-2 secure socket layer encryption for all data and documents at rest. Two-factor authentication via NIH Personal Identity Verification (PIV) card is required to log in to the system. The role-based access controls defined in the Administrative Controls are programmed into the system to secure PII data from view/access. Each administrator's access (i.e., Content Server administrator, Database Administrator (DBA), operating system administrator) is limited through role-based access to only those repositories where their expertise is required.

Physical controls are built into the Content Server product’s through automated enforcement

mechanisms. These mechanisms are provided and supported by the NIAID Office of Cyber Infrastructure and Computational Biology (OCICB) Operations and Engineering Branch (OEB). This branch is responsible for management of the servers, storage, databases, networks and operating systems used or accessed by NDRPAS.