US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/09/2025

OPDIV:

NIH

Name:

NIDDK Central Repository

PIA Unique Identifier:

P-6472293-623475

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.

Contractor

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

New Public Access

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

The system has replaced the NIH Identity, Credential, and Access Management (IAM) Services with the NIH Researcher Authorization Service (RAS) to facilitate user authentication. Password has been removed from the personally identifiable information (PII) collection. Also, system is adding the NIDDK Data Challenge Management (DCM) Platform and Analytics Hub that manages an online form for data challenges and prize competition.

Describe the purpose of the system.

The purpose of the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK) Central Repository (CR) is to expand study generated resources by supporting the receipt and distribution of data and biospecimens, enabling investigators not involved with the original work to test new hypotheses without the need to collect new data or biospecimens.

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

NIDDK-CR system collects and maintains data about its users including Full name, Username, User profile information (date account created, date of last login, user roles, study association and notification preferences), E-Mail Address, Phone and Fax Numbers, Shipping Address, Institutional Affiliation, resources' request information (request type, request status, project's title, objectives, analysis plan, research use statement, data security statement and policy compliance documentation, number of samples requested, data package requested, date of approval, voting status, date released, date of invoice, invoice number, purchase order number, date paid, user agreements, adherence and compliance with approved projects, extension dates, date data received, date samples received, request history), and maintains and shares information about the studies it holds (study name, description, objectives, outcome, public facing and non-public facing study documents, study data packages for distribution). In addition, the system stores and shares with its users study-specific data. These data are stored in limited data set (LDS) format and shared with its users in de-identified or coded format.

NIDDK-DCM Platform and Analytics Hub collects Full name, Email, Insititution, Job Title/Position, Team Name, Role in Team, Institutional Affiliation, Project Title, Project Description and Design, Analysis Plan.

NIDDK-CR makes data and biospecimens available from active and concluded clinical studies to the broader scientific community. The system has four major components, an archival of clinical data and associated documentation, a collection of biospecimens and associated inventory data, a web portal containing study-specific information, and linkage to sequencing data housed at the National Library of Medicine’s (NLM) National Center for Biotechnology Information' database of Genotypes and Phenotypes (dbGaP).

Users log in to the system using the NIH Researcher Auth Service (RAS). Using NIH RAS, users are able to authenticate using their NIH, eRA Commons, or Login.gov accounts. Users without an NIH or eRA Commons account, will use Login.gov. They will create an account with their preferred email address (organizational emails are required for access to the NIDDK-CR system, personal emails will be not be accepted), create a password, and establish Multi-factor authentication using one of the provided options. Each Identity Provider (IdP) is responsible for maintaining and verifying the user’s account per their respective requirements.

At initial login, NIH RAS will, with the user’s consent, provide the user’s profile information to the NIDDK-CR system including name, email, and organizational affiliation, when available. If only a subset of the required information is available, the user will enter the missing information in the NIDDK-CR system. All users are given default account permissions at registration and any additional NIDDK-CR system-specific roles are assigned by the contract support staff (Booz Allen Hamilton (BAH)).

NIDDK employees serve as the Contracting Officer's Representative (COR) and Project Manager (PM). They also review and approve the merit of requests, apply policy and provide oversight on the website utilization.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

TThe purpose of the NIDDK-CR is to expand study generated resources by supporting the receipt and distribution of data and biospecimens, enabling investigators not involved with the original work to test new hypotheses without the need to collect new data or biospecimens.

NIDDK-CR system collects and maintains data about its users including Full name, Username, User profile information (date account created, date of last login, user roles, study association and

notification preferences), E-Mail Address, Phone and Fax Numbers, Shipping Address, Institutional Affiliation, resources' request information (request type, request status, project's title, objectives, analysis plan, research use statement, data security statement and policy compliance documentation, number of samples requested, data package requested, date of approval, voting status, date released, date of invoice, invoice number, purchase order number, date paid, user agreements, adherence and compliance with approved projects, extension dates, date data received, date samples received, request history), and maintains and shares information about the studies it holds (study name, description, objectives, outcome, public facing and non-public facing study documents, study data packages for distribution). In addition, the system stores and shares with its users study-specific data. These data are stored in LDS format and shared with its users in de-identified or coded format.

NIDDK-DCM Platform and Analytics Hub collects Full name, Email, Insititution, Job Title/Position, Team Name, Role in Team, Institutional Affiliation, Project Title, Project Description and Design, Analysis Plan.

NIDDK-CR makes data and biospecimens available from active and concluded clinical studies to the broader scientific community. The system has four major components, an archival of clinical data and associated documentation, a collection of biospecimens and associated inventory data, a web portal containing study-specific information, and linkage to sequencing data housed at the NLM National Center for Biotechnology Information' dbGaP. dbGaP has its own Privacy Impact Assessment (PIA) including all legal authorities documented.

Users log in to the system using the NIH RAS. Using NIH RAS, users are able to authenticate using their NIH, eRA Commons, or Login.gov accounts. Users without an NIH or eRA Commons account, will use Login.gov. They will create an account with their preferred email address (organizational emails are required for access to the NIDDK-CR system, personal emails will be not be accepted), create a password, and establish Multi-factor authentication using one of the provided options. Each IdP is responsible for maintaining and verifying the user’s account per their respective requirements.

At initial login, NIH RAS will, with the user’s consent, provide the user’s profile information to the NIDDK-CR system including name, email, and organizational affiliation, when available. If only a subset of the required information is available, the user will enter the missing information in the NIDDK-CR system. All users are given default account permissions at registration and any additional NIDDK-CR system-specific roles are assigned by the contract support staff.

NIDDK employees serve as the Contracting Officer Representative and Project Manager. They also review and approve the merit of requests, apply policy and provide oversight on the website utilization

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
Institutional Affiliation/Organization, Fax number, Shipping Address
User Agreements/Material Transfer Agreements, Resources' request information, Country/Region, User profile information and Username
Study name, Description, Objectives, Outcome, Public-facing Study Documents, Study Data Packages for Distribution
Team Name, Role in Team, Project Title, Project Description and Design and Analysis Plan

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

Employees
Public Citizens
Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

5,000-9,999

For what primary purpose is the PII used?

To provide access to Central Repository data, and to participate in data challenges and prize competition.

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

To manage the study and generate resources held by NIDDK-CR.

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

Section 301 of the Public Health Service Act, describing the general powers and duties of the Public Health Service relating to research and investigation (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.

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

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Online
Government Sources
Within the DOC
Non-Federal Sources
Public
Commercial Data Broker
Private Sector

Identify the OMB information collection approval number and expiration date

Public Law 114-255, Section 2035, exempts research conducted by NIH from Paperwork Reduction Act (PRA) requirements. However, for the Data Challenge and Prize Competition the applicable OMB#0925-0740 expiration 11/30/2028.

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.

Access to PII data managed by NIDDK-CR direct contract support staff, currently Booz Allen Hamilton (BAH), authorized by information sharing agreement under contract (75N94021D00001/75N94021F00001).

Describe the procedures for accounting for disclosures.

Information maintained in NIDDK-CR is disclosed to the direct contractor managing the data to assist in the performance of their duties. Direct contractors who maintain records in this system are instructed to make no further disclosure of the records. Subject individuals may submit a written request to the NIDDK Privacy Coordinator or System Manager to obtain an accounting of 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.

Requesting resources from NIDDK-CR is voluntary. NIDDK-CR system users acknowledge collection of personally identifiable information (PII) when registering for an account to submit a request. When registering, users are presented with privacy and security notices, consistent with applicable federal laws and directives for accessing a government system.

In the case of study-specific indirect-PII, participants are notified at time of informed consent, consistent with current guidelines and regulations for future research use.

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.

System users may submit an inquiry to NIDDK-CR. In the case of study-specific indirect PII, participants are afforded opt-out/opt-in or tiered options for future research use. NIDDK-CR only stores and makes available resources which have been consented for future research use.

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

Requesting resources from NIDDK-CR is voluntary. By using the NIDDK-CR system, users consent to the collection of PII necessary to verify and authenticate a qualified user, and to process a request for resources. When major changes occur to the system, users are notified via email and/or automated messaging.

Significant changes relevant to study participants are provided by Study Staff at time of study-specific informed consent for future research use. NIDDK-CR does not have any direct identifiers to connect or communicate with study participants, therefore notification to study participants is outside NIDDK-CR scope of practice.

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.

Study participants, follow instructions provided by the Study Staff at time of informed consent. Resolution of individual concerns for study participants is outside NIDDK-CR scope of practice.

System users may submit an inquiry directly to NIDDK-CR support with specific concerns.

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

NIDDK-CR system direct contract support staff conducts routine audits of system users to confirm validity of accounts.

NIDDK-CR direct contract support staff curate study-level data upon receipt to confirm that only indirect participant information are included.

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.

Access to PII is assigned to personnel based upon current job responsibilities. The system uses specific login information to assign permissions/user roles which is considered PII.

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.

Access to PII is assigned to personnel based upon specified job responsibilities. The system uses specific login information to assign permissions/user roles which is considered PII.

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. Administrators and Privileged Users require additional training specific to their roles and responsibilities.

All NIDDK-CR direct contract support staff with access to PII or significant security responsibilities must complete role specific training and HHS/NIH applicable trainings. Direct contractors must undergo background checks, obtain badges, and sign Non-disclosure agreements (NDA).

Describe training system users receive (above and beyond general security and privacy awareness training).

Users requesting study-specific resources complete Good Clinical Practice, and Privacy and Data Security trainings as specified by their Institution/Center/Office (ICO).

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:

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. Intramural research records related to planning, development, oversight and execution of biomedical research projects and programs performed by NIH research staff, contractors or under collaborative research and development agreements (CRADAs).
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.
Disposition Authority Agency (DAA): DAA-0443-2012-0007-0003.

02-001: Official Case Files of Construction, Renovation, Endowment and Similar Grants
These records include, but are not limited to, records pertaining to the total application, progress reports, site visits, summary of review actions, award notices, terms and conditions of award, financial status reports, close-out documents, and other related papers maintained as an identifiable entity to be used in monitoring the use of supported space throughout the usage obligation.
Disposition: Cut off annually following completion of final grant-related activity that represents closing

of the case file (e.g., project period ended). Destroy 20 years after cutoff.
Disposition Authority: DAA-0443-2013-0004-0001

Study specific generated resource records are retained within the NIDDK-CR system in perpetuity or when no longer needed based on scientific research/advancements, whichever is longer.

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

Physical Controls: The information technology (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.

Administrative Controls: All technical personnel who access IT systems which contain protected information have met background investigation criteria, certifications, and requirements for their duties. Direct contractors have taken mandatory security and privacy training classes and annual refreshers.

Identify the publicly-available URL:

https://repository.niddk.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