US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/26/2024

OPDIV:

NIH

Name:

NIDDK GSS: NIDDK On-Site Web and Apps

PIA Unique Identifier:
P-4158428-500668

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.
In an effort to streamline the scope of the privacy impact assessment (PIA), applications and sites that share similar purpose and functionality have been consolidated under two distinct categories within this PIA:

1. SharePoint sites that were previously identified within the PIA are now consolidated under a single category: National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK)-managed SharePoint Sites.

2. Forms that were previously individually identified within the PIA are now consolidated under a single category: NIDDK Public Forms Site.

The remaining applications and sites include various NIDDK-managed and customized commercial-off-the-shelf (COTS) products which will continue to be individually documented due to their varied functionality.

In summary, On-Site Web and Apps now includes the following:

NIDDK-managed SharePoint Sites
NIDDK Public Forms Site
NIDDK Customized COTS:

a. Awards and Compensation Tool (ACT) (New)
b. Clinical Data Mart
c. Digital Pathology Repository
d. Globus
e. Integrated Research Data and Storage Application (iRDSA)
f. Jira/Intramural Administrative Management Branch (IAMB) Personnel Action Tracker (New)
g. Research Electronic Data Capture (REDCap) Production (Prod)
h. REDCap Survey

Describe the purpose of the system.

On-Site Web and Apps ("Applications") is a component of the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK) General Support System (GSS) and hosted by the NIDDK Computer Technology Branch (CTB) that reside on-premises at NIH.

On-Site Web and Apps provides automated mechanisms to facilitate the dissemination of information to the public for various NIDDK health areas; manage public registration, applicant reviews, and enrollment for all NIDDK workshops and training programs; and support internal operations and administrative functions.

The primary components within On-Site Web and Apps includes the NIDDK-managed SharePoint sites, NIDDK Public Forms Site, and several customized commercial off-the-shelf software (COTS) applications.

NIDDK-managed SharePoint sites provide a central collaborative platform to help manage and share content and knowledge related to the mission and objectives of NIDDK.

The NIDDK's Public Forms site includes a repository of publicly available electronic forms used to register for NIDDK sponsored events. A majority of the forms are used to determine the eligibility and quality of potential awardees for traineeships and mentorships in the NIDDK's Office of Minority Health Research Coordination (OMHRC) programs. OMHRC administers a variety of programs and initiatives to recruit high school students through post-doctoral educational level individuals into research training and mentorship programs to facilitate their development into future biomedical, behavioral, clinical, or social scientists.

NIDDK customized COTS products includes intranet and extranet applications primarily supporting NIDDK research efforts as well as personnel management.

The Awards and Compensation Tool (ACT) is an internal web application used by NIH staff and supervisors to streamline the collection and preparation of NIDDK federal employee annual performance and special act award nominations for submission to the NIH Office of Human Resources.

Clinical Data Mart is a database used to pull and restructure large amounts of the NIDDK clinical research data from the Clinical Centers Biomedical Translational Research Information System (BTRIS) system.

Digital Pathology Repository provides controlled access to deidentified whole slide images.

Globus, run by the University of Chicago, lets researchers share and access data on NIDDK or Globus storage systems from other institutions. NIDDK is currently sharing and receiving digital pathology whole slide images with a consortium that is receiving NIDDK grants.

Integrated Research Data and Storage Application (iRDSA) ensures that the data can be collected from across various sections of studies and will optimize the findings that lead to preventive measures or treatment modalities. It records all study associated data entered via REDCap.

Jira/ Intramural Administrative Management Branch (IAMB) Personnel Tracker is a project management tool used for tracking and routing NIDDK personnel information for hiring, placement and administrative personnel functions.

Research Electronic Data Capture (REDCap) Production (Prod) is a web-based data capture application that is accessible from within the NIH firewall. It is used for the development and management of online surveys and research databases.

REDCap Survey is a second installation of REDCap Prod that is available outside of the NIH firewall.

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

Collectively, NIDDK On Site Web and Apps manages the collection, storage and analysis of clinical, research and administrative data.

NIDDK Public Forms collect, maintain, and/or share the following information:
Name
Phone number
Mailing address
Email address
Education records
Employment status
Date Of Birth (DOB)
Ethnicity
Race

In addition, to the information collected from NIDDK Public Forms the following information is collected, maintained, and/or shared by NIDDK-managed SharePoint Sites:
Foreign activities
Medical notes
Bibliography
Age
Gender
Ethnicity
Race
Occupation
Curriculum vitae (CV)
Research initiatives and descriptions
Product use/ medication errors, and adverse events
Conference and Meeting Information (location, dates, speakers/presenters)

Budgetary Information

ACT collects NIH employee salary and performance information (e.g., Performance Management Appraisal Program (PMAP) scores)), names, emails, phone numbers, and employment status.

REDCap Production, REDCap Survey, and Clinical Data Mart collect name, driver’s license number, mother’s maiden name, email address, phone numbers, medical notes, certificates, education records, military status, foreign activities, DOB, photographic identifiers, vehicle identifiers, mailing address, medical records number, legal documents, device identifiers, employment status. In addition, the systems collect quantitative and qualitative data for clinical research.

The Digital Pathology Repository stores and shares digital whole slide images (WSI) of molecular and histopathological data sets so investigators can review and study pathology features and clinical diagnoses. Metadata in the WSI is de-identified and includes a slide barcode number, the clinical study number, the study site number, the organ biopsied (e.g., kidney or liver), the material (e.g., slide), tissue comment (e.g., biopsy), slide series number, and the participant study identification (ID) number (distinct from any patient's medical records numbers or personally identifiable information (PII)).

Integrated Research Data and Storage Application (iRDSA) collects name, email address, phone numbers, medical notes, DOB, medical records number (MRN), Medical notes (psychological questionnaire responses, and patient lab work (e.g., bone density, body composition, food intake)). iRDSA previously collected social security numbers (SSN) for tracking and management of payments for participation in clinical trials. SSNs are no longer available in iRDSA and are now maintained in the Clinical Research Information System (CRIS) Electronic Health Record (EHR) System, which maintains its own unique PIA on record.

Jira/ Intramural Administrative Management Branch (IAMB) Personnel Tracker does not directly collect information but manually inputs or uploads personnel information from various NIH administrative systems including Concur Government Edition (CGE), Fellowship Payment System (FPS), NIH Enterprise Directory (NED), NIH Facility Information Management System (FIMS), nSightHR and nSight for routing and tracking purposes. Information maintained by the tool includes Social Security Number, full name, email address, phone numbers, education records, military status, date of birth, photographic identifiers, mailing address, financial account info, legal documents, visa, employment status, passport number, demographics including age, marital status, and gender, travel details, and expenses.

Globus synchronizes and shares de-identified research data. No PII is handled by Globus.

Users access these applications using 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 softwar

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

On-Site Web and Apps provides automated mechanisms to facilitate the dissemination of information to the public for various NIDDK health areas; manage public registration, applicant reviews, and enrollment for all NIDDK workshops and training programs; and support internal operations and administrative functions.

The primary components within On-Site Web and Apps include:
NIDDK Public Forms Site -includes a repository of publicly available electronic forms used to register for NIDDK sponsored events.

NIDDK-managed SharePoint sites - a central collaborative platform to manage and share content and knowledge related to the mission and objectives of NIDDK.

NIDDK customized COTS products are intranet and extranet applications supporting NIDDK research efforts and personnel management. These include:
ACT
Clinical Data Mart
Digital Pathology Repository
Globus
iRDSA
Jira/iAMB
REDCap Prod
REDCap Survey

Collectively, NIDDK On Site Web and Apps manages the collection, storage and analysis of clinical, research and administrative data.
NIDDK Public Forms collect, maintain, and/or share the following information:
Name
Phone number
Mailing address
Email address
Education records
Employment status
Date Of Birth (DOB)
Ethnicity
Race

In addition, to the information collected from NIDDK Public Forms the following information is collected, maintained, and/or shared by NIDDK-managed SharePoint Sites:
Foreign activities
Medical notes
Bibliography
Age
Gender
Ethnicity
Race
Occupation
Curriculum vitae (CV)
Research initiatives and descriptions
Product use/ medication errors, and adverse events
Conference and Meeting Information (location, dates, speakers/presenters)
Budgetary Information

The COTS systems collect the following information:
ACT collects names, emails, phone numbers, NIH employee performance information (status, salary and Performance Management Appraisal Program (PMAP) data).

REDCap Production, REDCap Survey, and Clinical Data Mart collect name, driver's license number, mother's maiden name, email address, phone numbers, medical notes, certificates, education records, military status, foreign activities, DOB, photographic identifiers, vehicle identifiers, mailing address, medical records number, legal documents, device identifiers, employment status. In addition, the systems collect quantitative and qualitative data for clinical research.

The Digital Pathology Repository stores and shares digital whole slide images (WSI) of molecular and histopathological data sets for scientific review, including de-identified metadata (slide barcode number, the clinical study number, the study site number, the organ biopsied, the material (e.g., slide), tissue comment (e.g., biopsy), slide series number, and the participant study identification (ID) number (distinct from any patient's medical records numbers or PII)).

iRDSA collects name, email address, phone numbers, medical notes, DOB, medical records number (MRN), psychological questionnaire responses, and patient lab work (e.g., bone density, body composition, food intake). iRDSA previously collected social security numbers (SSN) for tracking and management of payments for participation in clinical trials. SSNs are no longer available in iRDSA and are maintained in the CRIS EHR System.

Jira/IAMB Personnel Tracker compiles personnel information for routing and tracking purposes. Information includes SSN, name, email address, phone numbers, education records, military status, DOB, photographic identifiers, mailing address, financial account info, legal documents, visa, employment status, passport number, demographics such as age, marital status, and gender, travel details, and expenses.

Globus synchronizes and shares de-identified research data. No PII is handled by Globus.
Users access these applications using NIH IAM Services which maintains its own PIA on record, including 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.

Research initiatives and descriptions, quantitative and qualitative data for clinical research, product use/medication errors, and adverse events

Digital WSI of molecular and histopathological data sets, including de-identified metadata in the WSI

Conference and Meeting Information (location, dates, speakers/presenters), Budgetary Information, travel details, and expenses.

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

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

To verify the identity and eligibility and correspond with applicants, and medical research participants, facilitate medical research, and tracking and routing NIDDK personnel for hiring, placement, and administrative personnel functions.

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.

42 US Code § 241/42 Code of Federal Regulations (CFR) Part 2a, 5 U.S. Code §¿301

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.

OPM/GOVT–1: General Personnel Records

09-25-0099 Clinical Research: Patient Medical Records

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

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

Office of Minority Health Research Coordination (OMHRC) Research Training and Mentor Programs Applications. OMB# 0925-0748, Expiration Date: 07/31/2026

OD/OPERA - 0925-0001- PHS Applications and Pre-Award Reporting Requirements (OD), Expiration Date: 01/31/2026.

OD/OPERA - 0925-0002 - Post-Award Reporting Requirements Including Research Performance Progress Report (RPPR) Collection (OD), Expiration Date: 01/31/2026.

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.

A Data Use Agreement (DUA) with the Porphyria Consortium of the Rare Diseases Clinical Research Network (RDCRN) is in place for any system users agreeing they will not attempt to identify patient participants in any research studies.

An Interconnection Security Agreement (ISA) is in place between NIDDK and the NCI. NCI provides IT support and assistance for a shared interface system and what data NCI can access.

Describe the procedures for accounting for disclosures.

For information within On-site Web and Apps that is held in a system of records, an accounting of disclosures is developed and maintained, including the date, nature, purpose of each disclosure, and the name and address, or other contact information of the individual or organization to which the disclosure was made. NIDDK retains the accounting of disclosures for the length of time the PII s maintained or five years after the disclosure is made, whichever is longer. NIDDK makes the accounting of disclosures available to the individual to whom the PII relates upon request.

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

For systems related to treatment of patients, study participants are provided an opportunity to sign a protocol consent form prior to any treatment and collection of data. Signature of the form expresses the participants explicit acknowledgement of the collection of PII. The protocol consent form explicitly addresses the use and distribution of the data with respect to confidentiality and the Privacy Act.

For systems not related to treatment of patients, end-users are notified at the point of entry that PII will be collected and stored.

Personnel information is not directly collected by applications or sites withing On-Site Web and Apps. However, it maintains information collected by other upstream sources which maintain their own unique PIA and have processes in place to notify individuals that their personal information will be collected.

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.

Individuals may decline or opt-out of the collection or use of their PII, however, submission of PII is a condition to being accepted into a research study, NIDDK sponsored programs or access to a NIDDK system. Applications or sites handling personnel records do not directly collection information from individuals. Upstream data sources, providing information to these personnel applications are responsible for establishing opt-out mechanisms for the use of PII.

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

In the event that a major change occurs to the system, individuals are to be contacted using data maintained in the system and asked to re-consent to any 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 may contact the program managers (administrators) who will contact the Institute/Center/Office (ICO) Privacy Coordinator and/or System Owner for resolution.

Study participants may contact the principal investigator, who will contact the ICO Privacy Coordinator and/or System Owner for resolution.

Individuals may also contact the NIH Privacy Office at Privacy@mail.nih.gov.

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 NIH IT Privacy Program requires system owners to implement privacy reviews and controls throughout the development life cycle, and to incorporate review of privacy controls into the annual assessment schedule of controls on all systems, networks and interconnected systems.

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.

The NIDDK employs a policy of least privilege in order to segregate data to only those employees, contractors, system and application roles to ensure that only those that "need to know" have access to the data. Access to PII data is controlled through defined role-based access controls.

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.

Technical, management and operational controls exist in order to allow those with access to PII to only access the minimum amount of information necessary required to perform their jobs. These controls include user identification, passwords, auditing, firewalls, encryption, intrusion detection systems, and Personal Identity Verification (PIV) cards. Least privilege access ensures that users are assigned to specific roles which limit the information required to perform the duties of the role.

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 use NIH applications must complete annual security awareness training. There are five categories of mandatory IT training (Information Security, Counterintelligence, Privacy Awareness, Records Management and Emergency Preparedness). Training is completed on the http://irtsectraining.nih.gov site with valid NIH credentials.

In addition, special roles such as system owners, managers, operators, program managers, developers and administrators are required to participate in specialized security awareness and privacy training based on job function and privileged access. Mandatory training includes - New Hire Records Management Awareness course; a records management course.

Users requiring remote access and/or administrative privileges must successfully complete those training sessions as well.

All users are required to read and agree to follow the NIH General Information Technology Rules of Behavior.

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

Role-based training is required at least annually--or more frequently as needed to address technology changes or patterns of vulnerabilities in information systems--for individuals with significant IT security responsibilities. This training is in addition to security awareness. NIH provides role-based training for the following job categories:

Managers: System Owners, Business/Data Owners, Data Stewards, Software Developers, Program Managers, Project Managers, Information System Security Officer (ISSO) and their information security employees or contractors

IT Administrators: Network, System and Database Administrators

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.

Item 01-001. Records of Intramural Research Projects of Historical Significance are retained and disposed of under the NIH Records Retention Schedule. Intramural research records relate 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). These records span the project lifecycle Disposition: Cut off annually at termination of project/program or when no longer needed for scientific reference. Transfer to the National Archives in five-year blocks when the newest records in the block are 15 years old.
DAA- 0443-2012-0007-0001

Item 01-003. Records of All Other Intramural Research Projects are retained and disposed of under the authority of the NIH Records Retention Schedule. These intramural research records relate 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). These records span the project lifecycle 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.
DAA-0443-2012-0007-0003

Item 03-001Records of Clinical Care Services are retained and disposed of under the authority of the NIH Records Retention Schedule. These records consist of clinical care services and clinical care department operational records that are consolidated under this one common temporary retention item. Disposition: Destroy 7 years after cutoff.
DAA–0443–2012–0007–0006

Item 03-002. Records of Radiology and Imaging are retained and disposed of under the authority of the NIH Records Retention Schedule. These records are comprised of X-rays and other roentgenographic images produced by devices and procedures, such as bodyhead scans created by computerized transaxial tomography (CT). Files may include physician interpretations of images/scans. Disposition: temporary records that can be destroyed 60 years after inactivity.
DAA–0443–2012–0007–0007

Item 03-005 Records of Patient Medical Records are retained and disposed of under the authority of the and NIH Records Retention Schedule. These records document admissions and medical treatment for a patient accepted in a research project. These records are the primary source of evaluation and analysis for either clinical care or clinical research study. Disposition: temporary records that can be destroyed when no longer needed for scientific reference.
DAA–0443–2012–0007–0010

Item 07-201. Systems and data security records are retained and disposed of under the authority of the NIH Records Retention Schedule. by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security and privacy controls throughout the life of the system, and NIH Record Schedule
DAA-GRS-2013-0006-0001

Item 06-211. Employee performance file system records are retained and disposed of under the authority of the National Archives and Records Administration (NARA) records retention schedule. Employee performance file system record. Performance records superseded through an administrative, judicial, or quasi-judicial procedure. Employee performance records are ratings of record, the performance plans on which ratings are based, supporting documentation for those ratings, and any other performance-related material required by an agency's performance appraisal system. Disposition: Destroy when superseded.
DAA-GRS-2017-0007-0011

Item 06-204. Official Personnel Folder (OPF)/Electronic OPF (eOPF) Long Term records are retained and disposed of under the authority of the Office of Personnel Management (OPM) Records Retention Schedule. The OPF (Standard Form 66) or its approved electronic equivalent documents an individual’s employment history. Records of separated employees saved

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

Administrative controls include system security plan, contingency plan, data/file back-up procedures, administrator training, and access based on least privilege principle. Privileged access is limited to the system administrators, programmers, and database administrators supporting specific applications or those assigned to support network devices and operations at the general support system level.

Technical access controls include user identification and authentication, through multi-factor authentication (including password and PIV card) firewall, NIH virtual private network (VPN), intrusion detection system (IDS), and encryption/public key infrastructure.

Physical controls include identification badges, key cards, cipher locks and closed-circuit television (TV).

Identify the publicly-available URL:

https://forms.niddk.nih.gov/
https://extranet.niddk.nih.gov
https://dkgbt.niddk.nih.gov
http://redcap.niddk.nih.gov/

The following links are only available during enrollment sessions and sent to attendees:
http://redcapsurvey.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