US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/11/2026

OPDIV:

NIH

Name:

Electronic Research Administration

PIA Unique Identifier:

P-9218201-570012

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

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

Alteration in Character of Data

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

There have been no updates since the last PIA. As a High Value Asset, the system is required to get the PIA updated annually.

Describe the purpose of the system.

The primary objective of eRA is to provide a government-wide solution to support end-to-end grants management activities. The integrated eRA system is comprised of Extramural Awards and Chartered Advisory Committees (IMPACII) and eRA Commons. IMPACII is internal facing and is used by the National Institutes of Health and eRA's partner agencies. eRA Commons is a portal for applicants and awardees to check on the status of their applications and awards and to submit additional information to the funding agencies throughout the lifecycle of the award. eRA also supports system-to-system communications with research institutions and service providers. IMPACII interfaces with Grants.gov, the central federal portal for posting funding opportunities and

for potential applicants to find funding opportunities and submit applications. IMPACII also interfaces with three (3) financial systems, the National Institutes of Health Business System (NBS), the Department of Commerce's Business Application System (BAS), and HHS' Unified Financial Management System (UFMS).

In addition to grants, the system also allows NIH and its Federal partners to manage other types of awards such as cooperative agreements, loan repayments, prizes, contracts, and other transactions.

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

The type of information eRA collects, stores and shares includes the following personally identifiable information (PII): name, e-mail address, phone numbers, education information, mailing address, demographic information, sex, date of birth (DoB), disability, disadvantaged background, persistent digital identifiers, current position, affiliated organization, service pay-back obligations, employment data, professional performance and credentialing history of licensed health professionals; professional and research misconduct case files, financial data including loan balances, deferment, forbearance, and repayment/delinquent/default status information; and Social Security Numbers (SSN) (full and last 4).

eRA supports the full award life cycle and is used by applicants and awardees worldwide. Listed below are the categories of individuals, with pre-award and award management records collected about them:

Applicants for or Awardees of awards - pre-award and award management (awardees) information;

Individuals named in applications, or awards, pre-award, and award management (awardees) information;

Referees - pre-award information;

Reviewers - pre-award information;

Academic medical faculty, pre- and post-doctoral medical students, and resident physicians - award management information.

Certificates of Confidentiality (CoC)s that are issued by NIH to protect the privacy of research subjects associated with research projects.

eRA has implemented role-based access controls which limits administration and functional user privileges.

Authentication uses 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.

eRA maintains roles assigned to individuals or users of the system including external users, as well as Federal staff, contractors, and special government employees. The system also maintains records of actions performed which can be used to perform workload analysis and assisted investigations.

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

The primary objective of eRA is to provide a government-wide solution to support end-to-end grants management activities. The integrated eRA system is comprised of Extramural Awards and Chartered Advisory Committees (IMPACII) that supports functionality for NIH and partner agency staff, and eRA Commons which is a portal for applicants and awardees to check on the status of their applications and awards, and to submit additional information to the awarding agencies throughout the lifecycle of the award. Both IMPACII and eRA Commons consist of multiple modules using a common database. eRA also supports system-to-system communications with research institutions and service providers. IMPACII interfaces with grants.gov, the central federal portal for posting funding opportunities and for research scientists to find grant opportunities and submit applications IMPACII also interfaces with three (3) financial systems, the National Institutes of Health Business System (NBS), the Department of Commerce's Business Application System (BAS), and HHS' Unified Financial Management System (UFMS).

In addition to grants, the system also allows NIH and its Federal partners to manage other types of awards such as cooperative agreements, loan repayments, prizes, contracts, and other transactions.

The type of information eRA collects, stores and shares includes the following personally identifiable information (PII): name, e-mail address, phone numbers, education information, mailing address, demographic information, sex, date of birth (DoB), disability, disadvantaged background, persistent digital identifiers, current position, affiliated organization, service pay-back obligations, employment data, professional performance and credentialing history of licensed health professionals; professional and research misconduct case files, financial data including loan balances, deferment, forbearance, and repayment/delinquent/default status information; and Social Security Numbers (SSN) (full and last 4).

eRA supports the full award life cycle and is used by applicants and awardees worldwide. Listed below are the categories of individuals, with pre-award and award management records collected about them:

Applicants for or Awardees of awards - pre-award and award management (awardees) information;

Individuals named in applications, or awards, pre-award, and award management (awardees) information;

Referees - pre-award information;

Reviewers - pre-award information;

Academic medical faculty, pre- and post-doctoral medical students, and resident physicians - award management information.

CoCs that are issued by NIH to protect the privacy of research subjects associated with research projects.

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
E-Mail Address
Mailing Address
Phone Numbers
Education Records
disability, persistent digital identifiers
disadvantaged background, usernames and passwords
current position, affiliated organization
sex, demographic information , professional performance and credential history
Service payback obligation, financial data, employment data

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

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

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purposes of PII entered into eRA modules are:

To support award programs and related process for NIH and other Agencies using the system, including (1) application preparation, receipt, referral, and assignment; (2) initial and council reviews; (3) award processing, funding, monitoring, and close-out; and (4) data querying, reporting, tracking, compliance, evaluation, audit, and communications.

To communicate matters related to agency award programs with (1) applicant organizations, including associated systems or system providers; (2) applicant or awardee persons such as the authorized institutional representatives, principal investigator(s) or trainees and individuals named in applications, awards, or progress reports; (3) reviewers; referees or (4) other entities such as Congress; federal departments or agencies, non-federal agencies or entities, or the general public; (5) identify persons who have requested a CoC and have been issued one; (6) assist NIH officials in maintaining the electronic record of CoC issued.

To maintain communication with former fellows and trainees who have incurred a payback obligation through the National Research Service Award Program and other federal research training programs.

To maintain official administrative files of application and agency-funded research and other programs.

To manage award portfolios.

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

To track individual trainees who receive support through grants such as fellowship or career awards

or who are supported through institutional training grant awards. Included are individuals in training for research and development supported in an investigator's laboratory that has an NIH-funded award (e.g., NIH Research Project Grants Program); these trainees are defined as "closely associated trainees."

To monitor the operation of review and award processes to detect and deal appropriately with any instances of real or apparent inequities.

To provide Congressional or otherwise mandated reports in compliance with statutory, regulatory, and policy requirements.

As an enterprise system and HHS Center of Excellence, eRA uses aggregate data (including some PII) for the following internal evaluation purposes: trend analysis, budget, and business forecasting.

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

The legal authorities to operate and maintain this Privacy Act records system are:
5 U.S. Code §301- U.S. Government Organization and Employees - Departmental Regulations
42 U.S.C. §§ 217a- Public Health Service Act - Advisory councils or committees
42 U.S.C. §§ 241 - Public Health Service Act Research and Investigations
42 U.S.C. §§ 281 - Public Health Service Act, Organization of the National Institutes of Health
42 U.S.C. §§ 282 Public Health Service Act Director NIH,
42 U.S.C. §§ 284 Public Health Service Act, Directors of National Research Institutes
42 U.S.C. §§ 284a Public Health Service Act Advisory Councils,
42 U.S.C. §§ 288 Public Health Service Act Kirschstein National Research Service Awards
42 U.S. Code § 288-1 - Intramural loan repayment program
42 U.S. Code § 288-2 - Extramural loan repayment program
44 U.S.C. §§ 3101 Presidential Review of Records, Records Management by Agency Heads
35 U.S.C. § 200-212 Patent Rights in inventions made with Federal Assistance,
48 C.F.R. Subpart 15.3 Source Selection in competitive negotiated acquisitions
and 37 C.F.R. 401.1-16 Bayh-Dole Act
44 U.S.C. Sec. 2904 General Responsibilities for Records Management
44 U.S.C. Sec. 2906 Inspection of Agency Records

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.

09-25-0223 "Records Related to Research Misconduct Proceedings"

09-25-0036 "NIH Extramural Awards and Chartered Advisory Committee (IMPAC II), Contract

09-25-0225 "NIH Electronic Research Administration (eRA) Records, HHS/NIH/OD/OER

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains
Hardcopy
Online
Government Sources
Within OpDiv
Other HHS OpDiv
Other Federal Entities
Non-Government Sources
Public

Identify the OMB information collection approval number and expiration date

OMB# 0925-0001 Expiration Date:12/31/2027
OMB# 0925-0002 Expiration Date: 11/30/2027
OMB# 0925-0361 Expiration Date: 1/31/2026 (working on renewal)
OMB# 0925-0689 Expiration Date: 8/31/2028

Private Sector
Other

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.

eRA has established documented formal Interconnection Security Agreement t (ISA) relationships with partnering organizations. Those ISAs are listed in the NIH Enterprise, Governance, Risk Management and Compliance (eGRC): Joint Cybersecurity Authorization Management (JCAM) tool. eRA has ISAs with the following entities:

Grants.gov
NIH Business System (NBS)
NIH Office of Financial Management (OFM)
NIH National Institute of Environmental Health Sciences (NIEHS)
HHS Payment Management System (PMS)
Unified Financial Management System (UFMS)
Veterans Administration (VA)
GrantSolutions
DoD (USAMRMC-CDMRP)
iEdison (NIST)
HHS Business Intelligence Information System (BIIS)
Department of Commerce (multiple systems)

Describe the procedures for accounting for disclosures.

All disclosures required by the Freedom of Information Act are logged by the Freedom of Information Act Office of the NIH Office of the Director. The log contains the following fields: name and address of requester, institution/organization, date requested, purpose of the request/the use of the information, release of PII (yes or no), if released the nature of the release (e.g., electronic, paper), name of recipient and address of recipient if different than the requester.

Per language in the eRA Partner Agreements and Interconnection Security Agreements (ISAs), parties are required to report privacy breaches or suspected breaches to eRA within one (1) hour of detection.

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

Individuals are provided a privacy disclosure notice when accessing eRA modules. A privacy notice informs the individual that 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 opt-out of collection of the collection of their PII by not registering with eRA, initiating an account and an awardee request. However, by doing so they will not be able to participate in the award program and/or log into eRA.

Demographic information allows a "do not wish to provide" option for individuals.

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

An amended Statement of Record Notice (SORN) will be published in the Federal Register to provide notice of any significant revision.

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 requesting clarification or voicing concerns about the use of their PII may make amendment requests addressed to the System Manager, Office of Extramural Research (OER) Privacy Coordinator, or NIH Senior Official for Privacy. They must reasonably identify the record and specify the information being contested, state the corrective action sought and the reason(s) for requesting the correction, and provide supporting information.

The right to contest records is limited to information that is factually inaccurate, incomplete, irrelevant, or untimely (obsolete).

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

PII is obtained from the subject individual. They have unlimited access to the system to update or correct the information or to change their decision regarding whether to provide demographic data.

eRA performs regression testing to ensure functionality with every release to ensure PII is not compromised. eRA has reduced the PII collected as data and for display on forms within Commons. The OER policy office clears data collection efforts via OMB annually.

In addition, the integrity, availability, and relevancy of PII in eRA is maintained via:
Daily and weekly backups.
Real-Time Data replication to an offsite location certified by NIH
Daily reviewed audit reports to determine if any unauthorized user(s) have accessed the system and/or database and if any system parameters have been modified without prior authorization on system and/or database
Annual recertification of users via designated NIH Institute, Center, or Office Coordinator.
Accounts identified as no longer required are deactivated
Access to eRA applications is restricted to encryption with Hypertext Transfer Protocol Secure (HTTPS).

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 is strictly limited according to the principle of least privilege, which means giving a user only those privileges which are essential to that user's work.

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.

eRA has implemented role-based access controls which limits administration and functional user privileges. Role based access has been implemented across eRA. Privacy and Security controls ensure proper protection of information by 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).

System users are provided guidance about proper usage of PII and privacy awareness. Agency users are also required to agree to the eRA Rules of Behavior and Data Access Agreements.

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 02-001 (DAA-0443-2013-0004-0001)
Official case files of construction, renovation, endowment and similar grants.
Disposition: Temporary. 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 cut-off;

Item 02-005 (DAA-0443-2019-0008)
Official Case Files of Applications and Awards, Appeals, and Litigation Records for Grants, Cooperative Agreements, and Other Transaction Activities
Disposition: Temporary. Cut off annually following completion of final award-related activity that represents closing of the case file (e.g., end of project period, completed final peer review, litigation or appeal proceeding concluded). Destroy 30 years after cut-off;

Item 02-003 (DAA-0443-2013-0004-0003)
Animal welfare assurance files.
Disposition: Temporary. Cut off annually following closing of the case file. Destroy 4 years after cut-off; and,

Item 02-004 (DAA-0443-2013-0004-0004)
Extramural program and grants management oversight records.
Disposition: Temporary. Cut off annually. Destroy 3 years after cut-off.

Item 04-401, Research Support for Certificates of Confidentiality - Support Documentation (DAA-0443-2017-0001-0001), Cut off annually at expiration of Certificate of Confidentiality. Destroy 6 years after cutoff.

Item 04-402, Research Support for Certificates of Confidentiality - Issued Certificates of Confidentiality (DAA-0443-2017-0001-0002), Cut off annually after all of the individually identifiable data from the research project have been destroyed, used, or otherwise are no long remaining in the NIH intramural program. Destroy 3 years after cutoff.

Item 04-403, Research Support for Certificates of Confidentiality - Issued Certificates of Confidentiality - For Extramural and Outside Research (DAA-0443-2017-0001-0003), Cut off annually at expiration of the Certificate of Confidentiality. Destroy 6 year(s) after cutoff.

Item 04-404, Research Support for Certificates of Confidentiality- Denied Certificates of Confidentiality (DAA-0443-2017-0001-0004),
Cut off annually at notification of denial. Destroy 3 year(s) after cutoff.

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

Administrative Controls:

To ensure proper protection of information and information technology systems include, but are not limited to, the completion of an Assessment and Authorization (A&A) package, Privacy Impact Assessment (PIA), Mandatory annual NIH Information Security and Privacy Awareness training or comparable specific in-kind training offered by participating agencies that has been reviewed and accepted by the NIH eRA Information Systems Security Officer (ISSO).

When the design, development, or operation of a system of records on individuals is required to accomplish an agency function, the applicable Privacy Act Federal Acquisition Regulation (FAR) clauses are inserted in solicitations and contracts.

Physical Controls:

To secure data and protect paper and electronic records, buildings, and related infrastructure against threats associated with their physical environment include, but are not limited to, the use of the HHS Employee Personal Identity Verification (PIV) ID and/or badge number and NIH key cards, security guards, cipher locks, biometrics, and closed-circuit TV. Paper records are secured under conditions that require at least two locks to access, such as in locked file cabinets that are contained in locked offices or facilities. Electronic media are kept on secure servers or computer systems.

Technical Controls:

eRA data is encrypted in transit, in use, and at rest.
Controls executed by the computer system are employed to minimize the possibility of unauthorized access, use, or dissemination of the data in the system. They include, but are not limited to user identification, password protection, firewalls, virtual private network, encryption, intrusion detection system, common access cards, smart cards, biometrics, and public key infrastructure.

Identify the publicly-available URL:

https://public.era.nih.gov/commons
https://grants.nih.gov/policy/humansubjects/coc.htm

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:

N/A

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