US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/16/2016

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

Additional updates to the eRA environment have taken place since the last PIA was approved. The Information Systems Security Officer (ISSO) Point of Contact (POC) has changed.

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

To enhance infrastructure security, eRA has deployed an alternate processing site which replicates production database data. For security reasons, the location is not provided.

Describe the purpose of the system.

The Electronic Research Administration (eRA) provides critical Information Technology (IT) infrastructure to manage over $30 billion in research and non-research grants awarded annually by NIH and other grantor agencies in support of the collective mission of improving human health.

eRA is recognized as an NIH Enterprise System and is a designated Center of Excellence by the U. S. Department of Health and Human Services (HHS). eRA is used as a grants management line of business system by other federal agencies to manage their award records. eRA systems align with

Grants.gov (the one-stop Web portal for finding and applying for federal grants), allowing for full electronic processing of grant applications from application submission through closeout of the grant award.

The purpose of eRA is to provide information technology solutions and support for the full life cycle of grants administration functions for the NIH as well as other federal operating divisions and agencies, including the:

Agency for Healthcare Research and Quality (AHRQ)
Centers for Disease Control and Prevention (CDC)
Food and Drug Administration (FDA)
Substance Abuse and Mental Health Services Administration (SAMHSA)
Veterans Health Administration (VA).

The eRA program is a component of the Office of Research Information Systems (ORIS) in the NIH Office of Extramural Research (OER), headquartered in Bethesda, Maryland. Additional program information can be found at the eRA home page, following this link, https://era.nih.gov/.

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

The eRA program facilitate grants administration support to NIH Institutes and Centers and to HHS agencies that fund extramural research. eRA acts as the information technology (IT) infrastructure for conducting interactive electronic transactions for the pre-award and award management of records.

To this purpose, the type of information eRA will request, collect, store and share includes personally identifiable information (PII) such as: name, e-mail address, phone numbers, education information, mailing address, financial account information, ethnicity, gender, and race.

eRA does not collect information (i.e. user credentials) about system users/administrators in order to control access. eRA has implemented role based access controls which limits administration and functional user privileges.

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

eRA systems, including eRA Commons, ASSIST and IMPAC II modules, support the full grants life cycle and are used by applicants and grantees worldwide.

eRA supports two main subsystems: "eRA Internal Applications" (also known as IMPAC II (Information for Management, Planning, Analysis, and Coordination), used by NIH staff, and "eRA External Applications" (Commons, iEdison), accessed by the grantee community through the Internet.

eRA includes a variety of pre-award and award management records that contain information needed to process applications and manage grant awards across the award lifecycle. Other eRA modules include eSubmission, RePORTER, databases, the NIH Data Book, an eRA intranet for federal staff, and QVR, a query retrieval tool.

Access to the system requires registration in the eRA "Commons". The individual is the source of the information about themselves and provides permissions to use that information in data collection and analysis. eRA does not collect information (i.e. user credentials) about system users/administrators in order to control access. eRA has implemented role based access controls which limits administration and functional user privileges.

Listed below are the categories of individuals mentioned above, matched 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;

Peer Reviewers - pre-award information;

Individuals required to report inventions, etc. - award management information; and

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

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

Yes

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

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Notes

Financial Accounts Info

Education Records

Ethnicity

Gender

Race

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

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Awardee Institutions and or Key Personnel

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of Personally Identifiable Information (PII) entered into eRA modules is for NIH grant proposal submission and administration business processes. When a user account is established at the request of the individual, PII is requested about users in the roles of applicants, awardees of the institutional organization staff and or key personnel. Submission of PII is voluntary; however, in order to process a transaction, most fields are required.

The records contained within this system will pertain to the following categories of individuals:

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;

Peer Reviewers - pre-award information;

Individuals required to report inventions, etc. - award management information; and,

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

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

As an NIH enterprise system and HHS Center of Excellence, eRA uses aggregate data (including some PII) for internal evaluation purposes: including 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
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.

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

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

SORN is In Progress

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other HHS OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Other

Identify the OMB information collection approval number and expiration date

OMB # 0925-0001 Expiration Date:10/31/2018
OMB # 0925-0002 Expiration Date:10/31/2018

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

Personally Identifiable Information (PII) entered into eRA modules is used for NIH grant proposal submission and administration business processes. When a user account is established at the request of the individual, PII is requested about users in the roles of applicants, awardees of the institutional organization staff and or key personnel. Submission of PII is voluntary; however, in order to process a transaction, most fields are required.

PII is shared with the following federal entities, within the constraints of the applicable System of Record Notice (SORN):

Agency for Healthcare Research and Quality (AHRQ)
Centers for Disease Control and Prevention (CDC)
Food and Drug Administration (FDA)
Substance Abuse and Mental Health Services Administration (SAMHSA)

Other Federal Agencies

See routine uses identified in NIH SORNs 09-25-0225 and 09-25-0036

State or Local Agencies

See routine uses identified in NIH SORNs 09-25-0225 and 09-25-0036

Private Sector

See routine uses identified in NIH SORNs 09-25-0225 and 09-25-0036

Describe any agreements in place that authorizes the information sharing or disclosure.

eRA has established documented formal Information Sharing Agreement (ISA) relationships with partnering organizations. Those ISAs are listed in the NIH System Authorization Tool (NSAT). eRA has ISAs with the following entities:

Agency for Healthcare Research and Quality (AHRQ)
Centers for Disease Control and Prevention (CDC)
Food and Drug Administration (FDA)
Grants.gov
NIH Business System
NIH Integrated Service Center
Substance Abuse and Mental Health Services Administration (SAMHSA)
Unified Financial Management System (UFMS)
Veterans Health Administration (VA)
eRA-DoD (USAMRMC-CDMRP) Interconnection
eRA-and-Grants.gov Program Management Office Interconnection

Describe the procedures for accounting for disclosures.

There is no release beyond those described in SORNs 09-25-0225, 09-25-0036, or subject to the Freedom of Information Act.

However, all requests for PII outside of HHS that are noted in the SORN and institutional officials at the parent institution of the individual (e.g. university, research facility, etc.) will be logged onto an Excel spreadsheet entitled Privacy Log maintained by the Office of Extramural Research Privacy Coordinator. The spreadsheet 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.

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 opt-out of collection of personal information by not registering with commons, initiating an account and awardee request.

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

An altered Statement of Record Notice (SORN) will be published in the Federal Register to provide notice of any significant revision. Additionally NIH has another mechanism, such as the NIH Guide, where it posts notices of new policies. NIH is required to maintain contact information for active grantees and those that have had recent research activities with NIH; therefore, an email blast is possible. However, NIH cannot control the accuracy of contact information of those persons that no longer have an active relationship with NIH.

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.

CONTESTING RECORD PROCEDURE (REDRESS):

Certain material will be exempt from amendment; however, consideration will be given to all amendment requests addressed to the System Manager. Individuals whose information is contained in the records can write to the System Manager identified in SORN 09-25-0036 and/or 09-25-0225, 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).

NIH has published a Notice of Proposed Rulemaking (NPRM), which is proposing to exempt confidential source-identifying material in a new system of records. This system of records relates to material that would inappropriately reveal the identities of referees who provide letters of recommendation and peer reviewers who provide written evaluative input and recommendations to NIH about particular funding applications.

These participants have received an express promise by the government that their identities in association with the written work products they authored and provided to the government will be kept confidential from certain requirements of the Privacy Act, as permitted by 5 U.S.C. § 552a(k)(5); specifically, from the provisions pertaining to providing an accounting of disclosures, access and amendment, notification, procedures and rules.

The exemptions and the promises of confidentiality are necessary to protect the integrity of NIH extramural peer review and award processes and ensure that the NIH efforts to obtain accurate and objective assessments and evaluations of funding applications from referees and peer reviewers is not hindered.

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 through the eRA "Commons" to update or correct the information or to change their decision regarding use of the information as part of aggregate 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 policy office clears data collection efforts via OMB annually.

In addition, the integrity, availability, and relevancy of PII in eRA is maintained via:
Hourly, 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 HTTPS.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Users have access to PII they provided and will be able to update their PII only. Access to others PII is restricted.

Administrators:

Administrators have access to entire system to ensure they are operating efficiently, patching and other maintenance related activities are implemented.

Developers:

Developers have access to PII to develop new features and functionality to ensure data integrity and quality.

Contractors:

Contractors have access to PII to support users and to maintain system functionality.

Others:

Referees - pre-award information;
Peer Reviewers - pre-award information;
Individuals required to report inventions, etc. - award management information; and,
Academic medical faculty, medical students and resident physicians - award management information.

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 for Common, iEdison and IMPAC II. Controls to ensure proper protection of information and information technology systems include, but are not limited to the mandatory completion of:
Security Assessment and Authorization (SA&A) package
Privacy Impact Assessment (PIA)
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).

The SA&A package consists of a:

Security Categorization
e-Authentication Risk Assessment
System Security Plan
Evidence of Security Control Testing
Plan of Action and Milestones
Contingency Plan
Evidence of Contingency Plan Testing.

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.

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.

Mandatory Annual Information Security and Privacy Awareness training is required for all HHS and NIH users. This awareness training includes modules specifically regarding use of PII and safeguarding PII.

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.

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 in accordance with the NIH Records Control Schedule contained in NIH Manual Chapter 1743, "Keeping and Destroying Records," which provides these disposition periods:

Item E-0001 (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 E-0002 (DAA-0443-2013-0004-0002)
Official case files of funded grants, unfunded grants, and award applications, appeals and litigation records.
Disposition: Temporary. Cut off annually following completion of final grant-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 10 years after cut-off;

Item E-0003 (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 E-0004 (DAA-0443-2013-0004-0004)
Extramural program and grants management oversight records.
Disposition: Temporary. Cut off annually. Destroy 3 years after cut-off.

Refer to the NIH Manual Chapter for specific retention and disposition instructions:

http://www1.od. nih.gov/oma/manualchapters/management/1743

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

Administrative Safeguards:

Controls to ensure proper protection of information and information technology systems include, but are not limited to, the completion of a:
Security Assessment and Authorization (SA&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)

The SA&A package consists of a:
Security Categorization
e-Authentication Risk Assessment
System Security Plan
Evidence of Security Control Testing

Plan of Action and Milestones
Contingency Plan
Evidence of Contingency Plan Testing.

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 Safeguards:

Controls to secure the 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 Persona 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 Safeguards:

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

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.

Session Cookies that do not collect PII.

Persistent Cookies that do not collect PII.

Other technologies that do not collect PII:

N/A

Does the website have any information or pages directed at children under 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?

No