US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/25/2026

OPDIV:

NIH

Name:

ServiceNow CSM for User Support in OER

PIA Unique Identifier:

P-4866076-596417

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?

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

Alteration in Character of Data

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

Since the past PIA, the system now collects additional personally identifiable information data types for users to add to their profiles. OMB Clearance expiration dates have also been updated.

Describe the purpose of the system.

The ServiceNow Customer Service Management (CMS) for User Support in Office of Extramural Research (OER) (SN CSM OER) is a cloud-based customer service management solution utilized by the OER offices and the eRA (not an acronym) Service Desk to manage support inquiries and service requests. Tickets are created automatically and tracked to completion in the system, when customers, internal to NIH, Partner Agencies, and external users, send an email, or submit Online using the SN CSM OER portal. Agents create tickets when customers contact the various support groups by phone.

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

The tickets in SN CSM OER will include the following personally identifiable information (PII) user contact information (name, email, phone number) and usernames. User may also enter the last four digits of the social security number, and their date of birth with requests to update their profile. Additionally, descriptions of questions or issues and resolutions, which may contain grant related sensitive data. In addition, some tickets may have reports based on eRA data attached which may contain sensitive PII collected by the eRA system.

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

The ServiceNow Customer Service Management (CMS) for User Support in Office of Extramural Research (OER) (SN CSM OER) is a cloud-based customer service management solution utilized by the OER offices and the eRA (not an acronym) Service Desk to manage support inquiries and service requests. Tickets are created automatically and tracked to completion in the system, when customers, internal to NIH, Partner Agencies, and external users, send an email, or submit Online using the SN CSM OER portal. Agents create tickets when customers contact the various support groups by phone.

The tickets in SN CSM OER will include the following personally identifiable information (PII) user contact information (name, email, phone number) and usernames. User may also enter the last four digits of the social security number, and their date of birth with requests to update their profile. Additionally, descriptions of questions or issues and resolutions, which may contain grant related sensitive data. In addition, some tickets may have reports based on eRA data attached which may contain sensitive PII collected by the eRA system.

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
Phone Numbers
usernames

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

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

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

Documentation of the details of the request to facilitate the process for account related services that are implemented as a standard process by the eRA staff.

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

NA

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

5 U.S. Code §301- U.S. Government Organization and Employees - Departmental Regulations
42U.S.C. §§ 217a- Public Health Service Act - Advisory councils or committees
42U.S.C. §§ 241 - Public Health Service Act Research and Investigations
42U.S.C. §§ 281 - Public Health Service Act, Organization of the National Institutes of Health
42U.S.C. §§ 282 Public Health Service Act Director NIH,
42U.S.C. §§ 284 Public Health Service Act, Directors of National Research Institutes 4
2U.S.C. §§ 284a Public Health Service Act Advisory Councils, 42U.S.C. §§ 288 Public Health Service Act Kirschstein National Research Service Awards
42U.S. Code § 288-1 - Intramural loan repayment program
42U.S. Code § 288-2 - Extramural loan repayment program
44U.S.C. §§ 3101 Presidential Review of Records, Records Management by Agency Heads
35U.S.C. § 200-212 Patent Rights in inventions made with Federal Assistance,
48C.F.R. Subpart 15.3 Source Selection in competitive negotiated acquisition
37 C.F.R. 401.1-16 Bayh-Dole Act44 U.S.C. Sec. 2904 General Responsibilities for Records Management
44 U.S.C. Sec. 2906Inspection 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.

09-90-1901, HHS Correspondence, Comment, Customer Service, and Contact List Records

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
Email
Online
Other
Government Sources
Within OpDiv
Other HHS OpDiv
Other Federal Entities
Non-Governmental Sources
Public
Private Sector

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: In Progress, TBD
OMB #0925-0689 Expiration Date: 8/31/2028

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.

eRA, as the source system has a Inter-agency Agreement (IAA) and a Memorandum of Understanding (MOU) in place with each partner agency which includes data sharing guidelines. eRA maintains its own PIA.

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.

Special access (that still falls under SORN disclosures) are handled by the eRA Data Modeling and Statistical Analysis Branch following the OER Data Use and Data Access agreement process. These are all tracked.

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

Users who submit tickets by logging in to the system are given a privacy notice and a link to the Privacy Act Statement at the time since they utilize the Single Sign On via eRA internal and external login pages.

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.

There is no opt-out option. Individuals may decline to give their PII. However, in doing so, they will not be able to obtain help from the Service desk.

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

Users are either “Agents” who use the system to manage tickets (primarily end-user support tickets) or “end-users” who are using the system to submit support tickets. Agents are NIH staff who have access to PII in order to properly communicate with their end-users and process their requests. End-users PII is from the source system, eRA . eRA maintains its own process to notify individuals when a major change occurs. eRA maintains its own PIA.

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.

There is no process for periodic reviews. The contact information is derived from eRA (verbally obtained information must match eRA and is verified). eRA maintains processes for periodic reviews. eRA maintains its own PIA.

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 granted only to support personnel, administrators, and other team members within the OER, using role-based security and access controls. User access to data is determined by the user's job description and need-to-know.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

The principle of least privilege is observed during all phases of the information life cycle. There are security and privacy controls to protect the system and data. All data is stored and maintained in secure systems. User activity is monitored and logged to ensure only appropriate use of the system and data. All users accessing the system use multi-factor authentication and are authorized based on roles and privileges carefully managed by the ServiceNow software.

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).

NA

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.

11-301,Technical and administrative help desk operational records. Destroy1 year after resolved, or when no longer needed for business use, whichever is appropriate (DAA-GRS-2017-0001-0001).

11-501, Public customer service operations records Destroy1 year after resolved, or when no longer needed for business use, whichever is appropriate (DAA-GRS-2017-0002-0001).

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 a 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 a agency function, the applicable Privacy Act Federal Acquisition Regulation (FAR) clauses are

inserted in solicitations and contracts.

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.

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.

Identify the publicly-available URL:

https://www.era.nih.gov/need-help.

https://public.era.nih.gov/commonshelp

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?

No

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